AGENCIA DE PROTECCION DE DATOS

Memoria 2002

AGENCIA DE PROTECCION DE DATOS

Memoria 2002

© AGENCIA DE PROTECCIÓN DE DATOS

D.L.: M-43896-2003

NIPO: 052-03-002-8

Imprime: tf artes gráficas

Impreso en papel reciclado

Índice

[1] El texto íntegro de los documentos que se relacionan en este apartado aparece incluido en el CD-ROM que acompaña a la presente Memoria.

3. Consejo de Europa
   3.1. Recomendación (2002)9 del Comité de Ministros a los Estados miembros sobre la protección de datos personales recogidos y tratados a efectos de seguros
   3.2. Informe que contiene directrices para la protección de los individuos en relación con la recogida y procesado de datos mediante vigilancia por vídeo (2003)

Presentación

Después de que la Sentencia 292/2000, de 30 de noviembre, consagrara el derecho a la protección de datos de carácter personal como aquel que tiene todo ciudadano para disponer libremente de los mismos, desvinculándolo del derecho a la intimidad y configurándolo como un derecho fundamental independiente, se inició un proceso de notable aumento de las acciones llevadas a cabo por la Agencia de Protección de Datos, de cuyo crecimiento ya se hizo eco la Memoria correspondiente al año 2001.

Aunque la mayor parte de la actividad de la Agencia se desarrolló bajo el mandato de mi antecesor en el cargo, sin embargo la Memoria correspondiente al ejercicio 2002, que tengo el honor de presentar, introduce ciertas novedades de orden metodológico.

En primer lugar, se incluye al comienzo de la misma un apartado dedicado a dar una clara idea de qué es la Agencia de Protección de Datos a la luz de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, y del resto de la legislación reguladora de su régimen jurídico. Asimismo, se introduce un organigrama de la Agencia que, hasta ahora, no se había recogido en Memorias anteriores.

En segundo lugar, se ha optado por editar un CD Rom en el que se recoge el contenido íntegro de la presente Memoria, así como de los Anexos que se citan más adelante (códigos tipo, documentos de trabajo del Grupo del Artículo 29, e informes y recomendaciones del

Consejo de Europa), y que no se recogen en la versión impresa, pero sí en dicho CD al objeto de facilitar su consulta ágil y rigurosa.

También se observan en la Memoria 2002 algunos aspectos formales que creemos contribuyen a potenciar la imagen de rigor, objetividad e independencia de la Agencia de Protección de Datos. Se ha hecho un importante esfuerzo para crear una nueva imagen de identidad institucional de la Agencia, y ello ha de plasmarse también en la línea editorial de la Agencia. En este aspecto, el nuevo logotipo y el formato de la Memoria con la introducción de los colores institucionales, pretenden conseguir que cualquier lector que se acerque a nuestra Memoria pueda relacionarla inmediatamente con la Agencia de Protección de Datos y con los valores que representa.

Por primera vez desde la creación de la Agencia se va a poder consultar la Memoria 2002 a través de la nueva página en internet. Creemos que esto producirá un efecto multiplicador en la divulgación de sus contenidos, ya que, hasta ahora, solamente se podía acceder a ella en soporte papel o informático, al estar incluidas las Memorias en los Catálogos de Ficheros que se publican cada año.

Desde el punto de vista sustantivo, en la Memoria 2002, se recoge el mismo nivel de información que en los años anteriores, aunque se ha procurado aportar una mayor sistematización de contenidos.

Espero y deseo que la publicación de esta Memoria contribuya a informar a la sociedad de los principales desarrollos en materia de protección de datos de carácter personal, y a aumentar el grado de conocimiento de todos los ciudadanos sobre esta materia al recogerse en ella los criterios mantenidos por la Agencia de Protección de Datos y la actividad desarrollada durante el año 2002. Madrid, 24 de septiembre de 2003.

JOSÉ LUIS PIÑAR MAÑAS
Director de la Agencia de Protección de Datos

Estructura y funcionamiento de la Agencia de Protección de Datos

I. Naturaleza Jurídica

El art. 35 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), establece que *«La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones».*

Por su parte el Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos (en lo sucesivo EAPD), que continúa vigente en tanto no sea aprobado otro nuevo, completa la descripción de la naturaleza jurídica que realiza el citado art. 15 de la LOPD, señalando en su art. 1 que se trata de un ente público de los previstos en el art. 6.5 del Real Decreto Legislativo 1091/1988, de 23 de septiembre, que aprueba el Texto Refundido de la Ley General Presupuestaria. Este precepto fue derogado por la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado que, sin embargo, establece en su disposición adicional décima el régimen jurídico de determinados entes públicos, entre los que se encuentra la Agencia de Protección de Datos (en lo sucesivo APD).

Del marco normativo señalado en el párrafo anterior, se deduce la primera característica que identifica la naturaleza jurídica de la APD. Se trata de un ente público que continuará rigiéndose por su legislación específica y, supletoriamente, por la Ley de Organización y Funcionamiento de la Administración General del Estado. En consecuencia se regía por lo

entonces previsto en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal (en lo sucesivo LORTAD), hoy derogada por la LOPD, por lo establecido en el EAPD, y el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD (la disposición transitoria tercera de la LOPD prevé su vigencia en tanto no se oponga a su contenido) y la Resolución de la APD, de 30 de mayo de 2000, en lo relativo a los modelos de notificaciones para inscripción de ficheros en el Registro General de Protección de Datos.

Además la Ley 6/1997, al respetar la normativa específica de la APD, excepciona a este ente público, entre otros, del proceso de adaptación que recoge en su disposición transitoria tercera.

El art. 1.2 del EAPD dispone que la Agencia actúa con plena independencia de las Administraciones Publicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

A modo de recapitulación, la APD es un ente de derecho público del derogado art. 6.5 de la Ley General Presupuestaria, que no ha de adaptar su régimen jurídico a lo previsto en la Ley 6/1997, que se regula por su normativa específica, y que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

II. Régimen Jurídico Aplicable

En el apartado anterior, que hemos dedicado a delimitar la peculiar naturaleza jurídica de la APD, ha quedado especificado que la misma se regirá, con carácter preferente, por su normativa específica. Pasemos ahora a pormenorizar cuáles son los regímenes jurídicos de los diferentes ámbitos de actuación.

El art. 35 de la LOPD va enumerando los diferentes ámbitos de la siguiente manera:

- En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la LOPD y sus disposiciones de desarrollo, actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. De este modo el art. 35.2 de la LOPD, recoge lo establecido en el art. 2.2 de la citada Ley 30/1992, cuando establece que las entidades de derecho público sujetarán su actividad a dicha Ley cuando ejerzan potestades administrativas, sometiéndose en el resto de su actividad a lo que dispongan sus normas de creación.

- En sus adquisiciones patrimoniales y contratación se regirá por el derecho privado. A tal fin el art. 36 del EAPD establece que los contratos que celebre se regirán por el derecho privado, pero su adjudicación será acordada con respeto de los principios de publicidad y concurrencia.

- El régimen del personal que presta servicios en la APD, será el previsto en la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública y demás disposiciones de desarrollo, cuando se trate de funcionarios públicos, y en el Convenio Único para el personal laboral de la Administración General del Estado, aprobado por Resolución de la Dirección General de Trabajo de 24 de noviembre de 1998.

- Desde el punto de vista del Derecho Presupuestario, la APD incorpora su presupuesto dentro de los Presupuestos Generales del Estado. Así el art. 48.1, a) de la Ley General Presupuestaria establece que se integran en los mismos la totalidad de ingresos y gastos del resto de entes del sector público estatal a que se refería, hasta la entrada en vigor de la Ley de Organización y Funcionamiento de la Administración General del Estado, el art. 6.5 que, como ya hemos visto, era el caso de la APD.

  Dentro de la Ley de Presupuestos Generales del Estado de 2002, la APD es el órgano responsable de ejecutar el Programa Presupuestario 146-B *«Protección de Datos de Carácter Personal»,* para lo cual dispone de créditos dentro de la Sección Presupuestaria 13, Organismo Público 301, por una dotación total de cuatro millones trescientos diez mil quinientos diez (4.310.510) euros.

  Así mismo, en lo relativo al control de las actividades económicas y financieras de la Agencia hay que distinguir entre el control externo que ejerce el Tribunal de Cuentas y el control interno que realiza la Intervención General de la Administración del Estado. En relación con este último, el art. 33.3 del EAPD dispone que se ejercerá, de conformidad con lo dispuesto en el art. 17.1 de la Ley General Presupuestaria, con carácter permanente. Precisamente en relación con este asunto, el art. 99.3 de esta última Ley señala que los entes públicos, a que se refiere la disposición adicional décima que la Ley de Organización y Funcionamiento de la Administración General del Estado, es decir la que incluye a la APD, estarán sometidos al sistema de control de su gestión económico-financiera establecido en su Ley reguladora, y, en su defecto, al establecido para las entidades públicas empresariales.

  Por lo tanto, de acuerdo con lo señalado con anterioridad, la APD está sometida a control financiero permanente. Esto quiere decir que dicho control se ejerce por una Intervención Delegada, sin perjuicio de las actuaciones que a nivel central ejerce la propia Intervención General de la Administración del Estado. Dicho control financiero permanente se desarrolla de acuerdo con lo dispuesto en el Real Decreto 2188/1995, de 28 de diciembre, por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Administración del Estado, y en las Circulares de dicha Intervención General 1/1989, de 2 de enero, 2/1989, de 28 de abril, y 5/1992, de 14 de diciembre.

  En lo relativo al control externo que ejerce el Tribunal de Cuentas, a tenor de la Orden Ministerial de 1 de febrero de 1996, por la que se aprueba la Instrucción de Contabili-

dad para la Administración Institucional, se realiza por medio del informe de auditoría que efectúa la Intervención General de la Administración del Estado y acaba siendo remitido al citado Tribunal.

- La contabilidad de la Agencia se ajusta al Plan General de Contabilidad Pública, aprobado por Orden Ministerial de 6 de mayo de 1994. A tenor de dicho plan, la APD ha de elaborar sus cuentas anuales (Balance, Cuenta de Resultado Económico – Patrimonial, Estado de Liquidación del Presupuesto y Memoria), sobre las cuales la Intervención General de la Administración del Estado realiza un informe de auditoría antes de remitirlas al Tribunal de Cuentas. Finalmente, se publica en el Boletín Oficial del Estado un resumen de las cuentas anuales, a tenor de lo previsto en la Orden del Ministerio de Hacienda de 28 de junio de 2000. En el año 2002, se publicaron las cuentas anuales correspondientes al ejercicio 2001, por Resolución del Director de la Agencia de 10 de octubre de 2002. (B.O.E. N.º 260, de 30 de octubre de 2002).

III. Estructura y Funciones

1. Independencia Funcional

Antes de entrar a analizar la estructura orgánica básica de la APD, resulta capital traer a colación lo dispuesto en el art. 35.1 de la LOPD, ya que en él se reconoce el carácter de entidad independiente de la propia Agencia. Efectivamente, el citado precepto señala lo siguiente:

> *«La Agencia de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno».*

A mayor abundamiento, el art. 1.2 del EAPD dispone que:

> *«La Agencia de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia».*

2. Estructura Orgánica

La estructura orgánica básica de la APD se establece en el art. 11 de su Estatuto, que distingue los siguientes órganos:

- El Director.
- El Consejo Consultivo.
- El Registro General de Protección de Datos, en lo sucesivo RGPD.
- La Inspección de Datos, en los sucesivo SGID.
- La Secretaría General, en lo sucesivo SGAPD.

Además, para el ejercicio de sus funciones el Director de la APD es asistido por una Unidad de Apoyo integrada por el Adjunto al Director y el Gabinete Jurídico. Ésta Unidad realiza, entre otras funciones, las de asesoramiento jurídico, interpretación normativa, emisión de informes, e impulso y desarrollo de las relaciones internacionales de la Agencia.

2.1. El Director de la Agencia

A tenor del art. 36 de la LOPD, dirige la Agencia y ostenta la representación de la misma, ejerce sus funciones con plena independencia y objetividad. El Director de la APD, con rango de Subsecretario, desempeña su cargo con dedicación absoluta, plena independencia y total objetividad. No estará sujeto a instrucción de autoridad alguna. Deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

En el EAPD. se distinguen entre las funciones de dirección (art. 12) y las funciones de gestión (art. 13) que corresponden al Director de la Agencia, de la siguiente manera:

- Funciones de dirección en las que el Director dictará las resoluciones e instrucciones que se requieran en relación con las competencias que corresponden a la Agencia. Dentro de ellas, destacan las referentes a procedencia o improcedencia de las inscripciones en el RGPD, requerimientos a los responsables de los ficheros de titularidad privada para que subsanen deficiencias de los códigos-tipo, procedencia o improcedencia de la denegación del acceso a algunos ficheros automatizados, autorización o denegación de transferencias internacionales de datos a países con un nivel de protección no adecuado, adopción de medidas cautelares y acuerdos de iniciación en relación con el ejercicio de la potestad sancionadora respecto a responsables de ficheros privados, solicitud de incoación de expedientes disciplinarios contra los responsables de ficheros públicos, y autorización de entrada en los locales en que se hallen los ficheros con el fin de proceder a las inspecciones que sean pertinentes.

- Funciones de gestión en las que el Director actúa en relación con la ejecución de la actividad económico–financiera de la Agencia. A tal fin adjudica, formaliza y controla el seguimiento de los contratos de la Agencia, aprueba los gastos y ordena los pagos, ejerce el control económico–financiero de la Agencia, programa su gestión, elabora el anteproyecto de presupuesto, propone la relación de puestos de trabajo, aprueba la Memoria Anual de la Agencia y ordena la convocatoria de las reuniones del Consejo Consultivo. En relación con estas funciones el Director podrá delegar en el Secretario General todas ellas, salvo las que se refieren al control económico–financiero de la Agencia, a la aprobación de la Memoria Anual, y a la ordenación de las convocatorias del Consejo Consultivo. Por Resolución del Director de la APD de 24 de abril de 1998 se delegaron en el Secretario General diversas competencias.

Por su parte, el art. 37 de la LOPD confía a la APD otras funciones que se refieren al cumplimiento de la legislación sobre protección de datos, a la adecuación de los tratamiento a los principios de la ley y al informe preceptivo de los proyectos de disposiciones generales que desarrollen el contenido de la LOPD.

2.2. El Consejo Consultivo

El Consejo Consultivo es el órgano colegiado de asesoramiento del Director de la APD. A él le corresponde la función de emitir informe en relación con todas las cuestiones que le someta el Director, y podrá formular propuestas sobre temas relacionados con las materias de competencia de la APD.

Los miembros del Consejo serán propuestos de la siguiente forma:

- Un vocal por el Congreso de los Diputados.
- Un vocal por el Senado.
- Un vocal de la Administración General del Estado propuesto por el Ministro de Justicia.
- Un vocal de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos en su ámbito territorial.
- Un vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias.
- Un vocal por la Real Academia de la Historia.
- Un vocal por el Consejo de Universidades.
- Un vocal de los usuarios y consumidores propuesto por el Consejo de Consumidores y Usuarios.
- Un vocal del sector de ficheros privados propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

Actúa como Presidente del Consejo Consultivo el Director de la APD y como Secretario, con voz y sin voto, el Secretario General de la Agencia.

El Consejo Consultivo se reunirá cuando así lo decida el Director de la APD, que, en todo caso, lo convocará una vez cada seis meses. También se reunirá cuando así lo solicite la mayoría de sus miembros.

2.3. El Registro General de Protección de Datos

El Registro General de Protección de Datos es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación, oposición y cancelación, regulados en los artículos 14 a 16 de la LOPD.

Corresponde al Registro General de Protección de Datos:

- Instruir los expedientes de inscripción.
- Expedir certificaciones de los asientos.
- Publicar relación anual de los ficheros notificados e inscritos.

De conformidad con el artículo 39 de la citada Ley serán objeto de inscripción en el Registro:

a) Los ficheros de que sean titulares las Administraciones Públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones de transferencias internacionales.
d) Los códigos tipo.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

El contenido de la inscripción está regulado en el artículo 20 de la LOPD, para los ficheros de titularidad pública y en el artículo 26 para los ficheros de titularidad privada.

Además, por vía reglamentaria se ha regulado el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

La regulación normativa de las funciones que corresponden al Registro está recogida en las siguientes disposiciones:

- Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la LORTAD, y que continúa vigente a tenor de lo dispuesto en la disposición transitoria tercera de la LOPD.
- Resolución de 30 de mayo de 2000, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos.

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

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

- El responsable del fichero deberá efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos.
- La inscripción de un fichero de datos no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la Ley.
- La notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.
- La notificación de los ficheros al Registro supone, una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quienes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, oposición, rectificación y cancelación.

2.4. La Inspección de Datos

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

Función inspectora

La Inspección de Datos no está contemplada por la LOPD desde la vertiente orgánica, sino sólo desde la funcional, siendo el EAPD el que prevé que las funciones inherentes al ejerci-

cio de la potestad de inspección que el art. 40 de la LOPD atribuye a la Agencia, se ejerzan por un órgano específico y separado de los demás al frente del cual se sitúa a un funcionario con categoría de Subdirector General.

No añade el Estatuto nuevas precisiones sobre el estatuto personal de quienes se encuadran en este órgano a las ya contenidas en la LOPD, la cual dispone que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus cometidos (art. 40), de donde resulta que la inspección deberá ser desempeñada por funcionarios de carrera. El carácter de «autoridad pública» que el art. 40.2 LOPD atribuye a los Inspectores de Datos significa que las personas responsables de los ficheros y/o tratamientos que ofrezcan resistencia o cometan atentado contra dichos funcionarios/inspectores, podrían incurrir en su caso en responsabilidad penal, exigible conforme a la legislación penal, y en todo caso incurrirían en la responsabilidad administrativa prevista en el art. 44.3.j) de la LOPD, calificada como obstrucción al ejercicio de la función inspectora.

El Estatuto desarrolla el contenido de la potestad de inspección atribuida a la Agencia en el ya citado art. 40 de la LOPD, precisando la facultad de la Inspección de Datos para efectuar inspecciones de oficio, aunque pudieran tener su origen en una denuncia de las personas afectadas, y detallando el alcance concreto de su capacidad para requerir y obtener información, así como examinar *in situ* los ficheros y sistemas informáticos en los que se traten datos de carácter personal. En conjunto, se trata de una serie de facultades cuya finalidad es la de obtener información y, en su caso, pruebas sobre posibles incumplimientos de la LOPD, que permitan posteriormente al órgano decisorio incoar procedimientos sancionadores y adoptar, en su caso, las medidas pertinentes dirigidas a la cesación de actividades ilícitas en los términos previstos en los arts. 37.f) y 49 de dicha Ley.

Como lógico correlato de esta función inspectora, se impone a los funcionarios que la ejercen el deber de guardar secreto sobre las informaciones que conozcan en el ejercicio de tal función, incluso después de haber cesado en la misma (art. 40.2 in fine); deber cuyo incumplimiento generaría la oportuna responsabilidad disciplinaria mientras se conserve la relación de servicio con la APD, y que se reputaría infracción administrativa grave, una vez extinguida dicha relación, al amparo del art. 44.3 g) de la LOPD.

Función instructora

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

El ejercicio de esta función instructora correspondiente a la Subdirección General de Inspección de Datos, no es más que la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia (art. 37.g de la LOPD) y la necesaria garantía del procedimiento sancionador, cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas o órganos distintos (art. 134 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).

El procedimiento sancionador, de conformidad con lo previsto en el art. 48.1 de la LOPD, está regulado en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones, estructurándose como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución, correspondiendo al funcionario instructor el desarrollo completo de la fase de Instrucción u Ordenación del procedimiento y la propuesta razonada al Director de la Agencia de las otras dos, es decir, del acuerdo de inicio del procedimiento sancionador y de la Resolución del mismo.

Por otra parte, la función instructora se concreta en la incoación de tres clases de procedimientos: el procedimiento sancionador incoado contra los responsables de ficheros de titularidad privada por infracción de los principios y reglas contenidos en la LOPD; el procedimiento por infracciones de las Administraciones Públicas (art. 46) cuando es una Administración de esta clase la que vulnera los preceptos de la Ley; y el procedimiento de tutela de derechos previsto en el art. 18 de la Ley, que se actúa cuando son vulnerados los derechos de oposición, acceso, rectificación o cancelación de los afectados (arts. 15 a 17).

El procedimiento de tutela de derechos supone la existencia de un posible incumplimiento de la Ley que no sea constitutivo de infracción, lo que justifica referirse a esta potestad arbitral de tutela al margen de la potestad sancionadora de la APD. La nueva LOPD ha venido a reproducir el mismo esquema que regía bajo la vigencia de la derogada LORTAD, si bien ha introducido dos novedades en el procedimiento de tutela de derechos al ampliar el plazo máximo para dictar resolución a seis meses (art. 18.3 LOPD), siguiendo la pauta general que para los procedimientos administrativos establece el art. 42.2 la Ley 30/1992, de 26 de noviembre, y dar entrada en la regulación de estos procedimientos a un nuevo derecho que se desconocía en la anterior legislación: el derecho de oposición, que consiste en esencia en que aquellos casos en que no sea necesario el consentimiento del afectado para el tratamiento de sus 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 (art. 6.4).

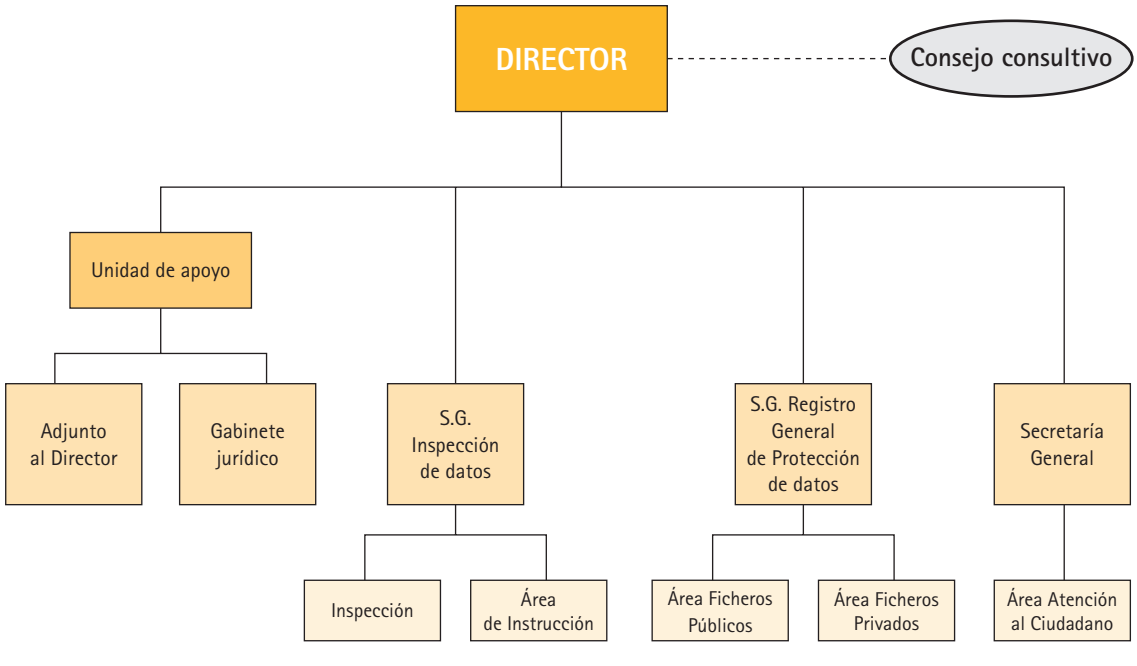
2.5. Secretaría General

A la Secretaría General, de acuerdo con lo dispuesto en los arts. 30 y 31 del EAPD, le corresponden las siguientes funciones:

- Funciones de apoyo y ejecución: Elaborar los informes y propuestas que les solicite el Director, notificar las resoluciones del Director, ejercer la secretaría del Consejo Consultivo, gestionar los medios personales y materiales, así como atender la gestión económico-administrativa de la APD, llevar el inventario, y cuantos asuntos no estén atribuidos a otros órganos de la APD.

- Otras funciones: Formar y actualizar el fondo de documentación en material de protección de datos, editar los repertorios oficiales de ficheros inscritos en el RGPD, las memorias anuales y cualesquiera otras publicaciones de la APD, organizar conferencias, seminarios y cualesquiera otras actividades de cooperación internacional e interregional sobre protección de datos y facilitar la información necesaria para llevar a cabo campañas de difusión a través de los medios de comunicación.

3. Organigrama de la Agencia



La Protección de Datos de Carácter Personal en España: Análisis y valoración

I. El Consejo Consultivo

De acuerdo con lo establecido en el artículo 38 de la LOPD, el Director de la Agencia estará asesorado por un Consejo Consultivo. Su funcionamiento se rige por lo previsto en la Sección 3ª del Capítulo III del Real Decreto 428/1993, de 26 de marzo, que aprueba el EAPD.

Sus cometidos son de naturaleza general, ya que emitirá informe sobre todas las cuestiones que someta a su consideración el Director de la Agencia. Así mismo, el Consejo podrá formular propuestas en relación a las competencias propias de la Agencia.

Durante el año 2002 se produjo la renovación del Consejo Consultivo por expiración del plazo de cuatro años establecido en el artículo 20,1 del EAPD. El anterior Consejo fue nombrado por Orden de la Ministra de Justicia de 6 de marzo de 1998, que dio publicidad al Acuerdo del Consejo de Ministros de 27 de febrero de 1998, y estaba compuesto por los siguiente vocales:

- Don Carlos Navarrete Merino, a propuesta del Congreso de los Diputados.
- Doña María Rosa Vindel López, a propuesta del Senado.
- Don Álvaro de la Cruz Gil, como vocal de la Administración Local, a propuesta de la Federación Española de Municipios y Provincia.
- Don Eloy Benito Ruano, a propuesta de la Real Academia de Historia.
- Don Antonio Pérez Prados, a propuesta del Consejo de Universidades.
- Doña Nuria Díaz Anduiza, como vocal de los usuarios y consumidores, a propuesta, en terna, del Consejo de Consumidores y Usuarios.

- Doña Elena Gómez del Pozuelo, como vocal del Sector de ficheros privados a propuesta, en terna, del Consejo Superior de Cámaras Oficiales de Comercio, Industria y Navegación.

Por Orden JUS/2636/2002, de 25 de octubre, se dispuso la publicación del Acuerdo del Consejo de Ministros de 18 de octubre de 2002, por la que se nombran los nuevos vocales del Consejo Consultivo de la Agencia de Protección de Datos. La composición quedó establecida así:

- Dª Carmen Matador de Matos, a propuesta del Congreso de los Diputados.
- D. Félix Lavilla Martínez, a propuesta del Senado.
- D. José Luis Piñar Mañas, como vocal de la Administración General del Estado, a propuesta del Ministro de Justicia.
- D. Antonio Troncoso Reigada, Director de la Agencia de la Comunidad de Madrid, a propuesta de la misma.
- D. Gonzalo Brun Brun, como vocal de la Administración Local, a propuesta de la Federación Española de Municipios y Provincia.
- D. Eloy Benito Ruano, a propuesta del Consejo de Universidades.
- D. Alejandro Perales Albert, como vocal de los consumidores y usuarios, a propuesta, en terna, del Consejo de Consumidores y Usuarios.
- Dª Belén Veleiro Reboredo, como vocal del sector de ficheros privados, a propuesta, en terna, del Consejo Superior de Cámaras Oficiales del Comercio, Industria y Navegación.

A tenor del artículo 22.3, del anteriormente citado Real Decreto 428/1993, actúa como Presidente del Consejo Consultivo el Director de la Agencia de Protección de Datos. Tales funciones fueron ejercidas por Don Juan Manuel Fernández López hasta que se produjo su cese por Real Decreto 1171/2002, de 8 de noviembre. Su puesto fue cubierto por D. José Luis Piñar Mañas que, hasta que se produjo el citado nombramiento por Real Decreto 1172/2002, de 8 de noviembre, era vocal del Consejo en representación de la Administración General del Estado.

La sesión constitutiva del nuevo Consejo Consultivo tuvo lugar el 6 de noviembre de 2002. Con fecha 3 de diciembre de 2002, se celebró la primera reunión presidida por el nuevo Presidente del Consejo Consultivo y Director de la Agencia de Protección de Datos, D. José Luis Piñar Mañas.

II. Subdirección General del Registro General de Protección de Datos

1. Introducción

El artículo 25 de la LOPD establece que se podrán crear ficheros de titularidad privada que contengan datos personales cuando resulten necesarios para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que la Ley establece para la protección de las personas.

De forma paralela, el artículo 20 dispone que las Administraciones Públicas sólo podrán crear ficheros por medio de disposición general publicada en el Boletín o Diario Oficial correspondiente. En efecto, en los de titularidad pública no basta la mera voluntad del responsable sino que se precisa norma habilitante.

En todo caso, toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. Así mismo, será obligatorio comunicar las variaciones que se produzcan en la finalidad, en su responsable y en la dirección de su ubicación o cualquier otra circunstancia que implique alguna variación en la información anotada registralmente.

El Registro General de Protección de Datos inscribirá el fichero o tratamiento si la notificación se ajusta a los requisitos previstos legalmente. Con la pretensión de evitar una perni-

ciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización o la inscripción constitutiva. En este sentido, el beneficio de la simplificación en los trámites administrativos en la inscripción de un fichero o tratamiento no afectan al nivel de protección garantizado ni a ninguna de las demás obligaciones derivadas de la LOPD.

La solicitud de inscripción de ficheros se deberá efectuar mediante los modelos establecidos en la Resolución de la Agencia de Protección de Datos, de 30 de mayo de 2000 (B.O.E. 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 solicitudes de inscripción en el Registro General de Protección de Datos. Estos modelos, así como el programa de ayuda para la generación de notificaciones, se pueden obtener a través de Internet en nuestra página *Web www.agpd.es*

La utilización del programa de ayuda, mencionado anteriormente, se obtiene de forma gratuita, permitiendo que los procesos de inscripción sean más eficaces y eficientes, minimizando los costes de recogida de la información, facilitando la depuración y calificación previa a la inscripción, consiguiendo el máximo control en todo el procedimiento. A su vez, facilita al responsable la cumplimentación del aspecto formal del documento dado que existe una herramienta de ayuda que le guía en la cumplimentación de los modelos de inscripción.

Por otra parte, la tramitación de la solicitud de inscripción se realiza sin coste alguno por parte de la Agencia de Protección de Datos.

La inscripción de ficheros durante el año 2002, ha estado caracterizada por la expiración de dos plazos. Uno relativo al plazo para implantar las medidas de seguridad de nivel alto y otro que afecta al período transitorio, establecido en la disposición adicional primera de la LOPD, para adecuar formalmente los ficheros automatizados preexistentes a la entrada en vigor de la Ley.

Respecto al plazo para la adopción de las medidas de seguridad de nivel alto, inicialmente establecido por el Reglamento de Seguridad, fue ampliado hasta el día 26 junio de 2002, 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.

El día 14 de enero de 2003 se cumplió el período transitorio establecido en la LOPD para que las Administraciones Públicas adecuen las disposiciones de creación de los ficheros existentes a las nuevas exigencias legales. Para dar cumplimiento a esta previsión algunas Administraciones Públicas ya comenzaron a realizar los trámites necesarios en años anteriores, sin embargo, en 2002 ha sido considerablemente superior el número de disposiciones que han sido publicadas a estos efectos.

La LORTAD, excluía de su ámbito de aplicación, en su artículo 2 apartado a) *«a los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general»* en su apartado c) *«a los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales»* en el apartado 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»* y en su apartado 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...*». Sin embargo, la LOPD ha incluido en su ámbito de aplicación estos tratamientos e, igualmente, el día 14 de enero de 2003, ha finalizado el plazo transitorio para declararlos.

De acuerdo con lo señalado en la STC 292/2000, se han continuado produciendo, durante 2002, un número significativo de notificaciones para adecuar la inscripción de ficheros de titularidad pública, concretamente en lo relativo al apartado de cesiones.

El paisaje del entramado empresarial y de las Administraciones Públicas está cambiando hacia estrategias de desarrollo de la gestión y administración electrónica y, de igual modo, el auge de la Sociedad de la Información lleva consigo el aumento exponencial en la creación de sistemas de información que desarrollan nuevos ficheros y tratamientos.

Durante 2002, se han recibido 35.697 solicitudes relacionadas con la inscripción de ficheros, lo que ha supuesto un aumento de más del 100%, con respecto a las solicitudes recibidas durante 2001. Este aumento se une a los producidos en los ejercicios de 1999, 2000 y 2001, por lo que, desde el año 1999 hasta el año 2002, se ha multiplicado por siete el número de solicitudes.

Estas solicitudes han representado un total de 77.029 operaciones de inscripción en el RGPD, de las cuales 73.081 lo fueron a solicitud del interesado (61.327 de nuevas inscripciones, 7.212 de modificación y 4.542 de supresión) y el resto, es decir, 3.948 han sido realizadas de oficio.

Así mismo, estas operaciones han supuesto la emisión de 76.035 documentos de salida de los cuales 68.416 son resoluciones de notificación de inscripción. Por otra parte, también se han generado otros 7.619 documentos de salida, de los que 5.804 han correspondido a requerimientos de subsanación de errores en las solicitudes de inscripción y 1.815 al envío de documentación relativa a la inscripción de ficheros.

Como consecuencia de todas estas operaciones de inscripción, a finales de 2002 constaban inscritos un total de 328.649 ficheros de titularidad pública y privada, frente a los 271.875 registrados al finalizar el 2001, lo que supone un aumento aproximado del 20%.

Este incremento parece indicar que, tanto el sector privado como las Administraciones Públicas, cada vez tienen más conciencia respecto al derecho fundamental de la protección de los datos personales que tratan en el desempeño del objeto legítimo de su actividad, en el caso de los tratamientos de titularidad privada, o en el desarrollo de las funciones que la Ley atribuye a las AAPP como titulares y órganos responsables de ficheros o tratamientos.

2. Derecho de consulta al Registro General de Protección de Datos

2.1. Introducción

De conformidad con el artículo 14 de la LOPD, el Registro General de Protección de Datos, como órgano integrado en la Agencia de Protección de Datos, garantizará la publicidad de los tratamientos, permitiendo que cualquier persona pueda conocer, recabando para tal fin la información oportuna del RGPD, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Los procedimientos de notificación tienen por objeto asegurar la publicidad de los ficheros, y el RGPD debe contribuir a la transparencia de los tratamientos de datos efectuados en territorio español.

Para poder garantizar a los ciudadanos el derecho de consulta será necesario que los responsables hayan cumplido con las previsiones de notificar los tratamientos.

Además, será necesario notificar las modificaciones que afecten a cualesquiera de los extremos exigidos en la notificación, en particular, aquellos relacionados con la identidad del responsable o con las variaciones de los datos consignados en el apartado de dirección de acceso a los efectos de que los datos registrales sean fiel reflejo de la situación actual y real del responsable.

2.2. Publicación del catálogo de ficheros

Para cumplir con la finalidad que recoge la Ley se publica, en la página web de la APD, con una actualización mensual, el catálogo de los ficheros inscritos en el RGPD. Durante 2002 se estima que se han realizado unas 80.000 consultas a dicho catálogo. Así mismo, se edita cada año un CD ROM que contiene la relación de ficheros inscritos hasta ese momento.

Además, se han tramitado 495 solicitudes de copia del contenido de la inscripción. La solicitud de la copia completa del contenido de la inscripción debe ser realizada por persona con representación suficiente del responsable del fichero, de conformidad con lo dispuesto en el artículo 32 de la LRJPAC.

Los recursos necesarios, tanto humanos como materiales, para atender estas solicitudes han sido importantes, teniendo en cuenta que cada solicitud de este tipo puede involucrar a tres ficheros como media, y que la copia completa del contenido de la inscripción consta de cinco páginas.

2.3. Información al responsable

Merece destacar, por su importancia, aquellas funciones del RGPD que implican una actividad de información y relación con los responsables de los ficheros, puesta de manifiesto mediante comunicaciones escritas en las que se les informa de aquellos aspectos que podrían resultar erróneos o incoherentes en las notificaciones presentadas. En otras ocasiones, esta función se ha realizado por vía telefónica, atendiéndose aproximadamente 15.000 consultas, relacionadas con los expedientes que estaban siendo tramitados o que se habían tramitado en su día, así como, otras en las que se solicitaba asesoramiento sobre la utilización del programa de ayuda para la generación de notificaciones.

También se han realizado en el ámbito de las Administraciones Públicas funciones de apoyo a la inscripción, informando y colaborando con los responsables de ficheros titularidad pública para facilitarles esta labor. Aunque estas tareas no se encuentren contabilizadas, dado que en muchas ocasiones se llevan a cabo mediante teléfono, correo electrónico y reuniones presenciales, sí que se debe señalar el esfuerzo añadido que ha supuesto para el personal de la Agencia su desarrollo, cuando, como se puede apreciar a lo largo de esta Memoria, el número de expedientes se ha visto incrementado considerablemente.

Otras veces, las comunicaciones telefónicas fueron realizadas por el personal del RGPD con el fin de obtener alguna aclaración o la subsanación de algún defecto con el fin de impulsar la ordenación del correspondiente procedimiento.

Durante el año 2002 se han notificado un total de 7.619 comunicaciones escritas, informando de diversos aspectos relacionados con la subsanación de errores en la notificación o con información relativa a la inscripción de ficheros. Esta cifra representa únicamente el 10% del total de escritos emitidos relativos a la inscripción de ficheros. El resto de los escritos de salida emitidos, 68.416, están relacionados con la notificación de las resoluciones del Director de la Agencia correspondientes a la inscripción, modificación o supresión de ficheros.

Estas cifras ponen de manifiesto que, en la gran mayoría de los casos, se procede a realizar la inscripción del fichero con la primera notificación presentada por los responsables. En este sentido, la utilización del programa de ayuda para la generación de notificaciones resulta de gran utilidad para agilizar el trámite de notificación y evitar errores en la cumplimentación del modelo de notificación, como ya se ha puesto de manifiesto en anteriores memorias.

Igualmente, aunque en número menor, debido a la falta de recursos humanos, se han mantenido reuniones con representantes de responsables de ficheros al estimarse más operativo, por alguna situación peculiar, afrontar de esta forma la situación relativa a la inscripción o adecuación de sus tratamientos. Así mismo, se han impartido diversos cursos, seminarios y conferencias sobre la inscripción de ficheros en diversas sedes tanto de universidades y entidades públicas como privadas.

3. Inscripción de Ficheros de Titularidad Privada

3.1. Evolución en la inscripción de ficheros de titularidad privada

Del total de operaciones realizadas en el RGPD, relativas a la inscripción de ficheros de titularidad privada (66.051) un 86% han sido altas, un 8% han sido operaciones de modificación, y el resto ha sido (6%) supresiones de inscripción.

Como consecuencia de las operaciones de inscripción realizadas, a 31 de diciembre de 2002 figuraban inscritos 292.755 ficheros de titularidad privada, es decir, 52.000 inscripciones más que al finalizar el año anterior. En 2001 figuraban 22.000 ficheros más inscritos con respecto al año 2000.

El fin del plazo transitorio para notificar la adecuación de los ficheros preexistentes, junto con la mayor difusión de las obligaciones derivadas de la LOPD ha propiciado que un gran número de los responsables que, hasta este momento, no hubieran notificado sus tratamientos, procedieran a cumplir con la obligación de notificar los tratamientos durante este período.

En esta toma de conciencia ha influido, además de la labor informativa llevada a cabo durante los últimos años por la APD, la efectuada por las organizaciones empresariales, colegios profesionales y consultores que han contribuido a acercar esta materia a los diferentes sectores.

A los sectores que tradicionalmente han tenido mayor repercusión en el tratamiento de datos personales como el bancario, asegurador, telecomunicaciones, marketing, etc., se han

añadido otros como la hostelería, construcción, actividades inmobiliarias, asesorías, venta y reparación de vehículos, oficinas de farmacia y establecimientos sanitarios.

Por lo que respecta a las operaciones realizadas de oficio, durante este período se han realizado un total de 2.837 operaciones de este tipo en inscripciones de titularidad privada. Estas operaciones han tenido como finalidad, por una parte, la subsanación de errores materiales y, por otra, la normalización de las denominaciones de las leyes que consignan en las declaraciones, así como las actualizaciones de las denominaciones sociales que figuran como responsables de los tratamientos. Además, se ha procedido a completar y normalizar las inscripciones de los ficheros no automatizados o manuales, ya que no existe ningún apartado en el modelo normalizado que diferencie el tipo de notificación por este concepto.

En este sentido, merecen mención especial las subsanaciones que se han realizado a las inscripciones cuyos responsables han notificado que los datos incluidos en el fichero procedían del censo promocional. Si bien esta procedencia se encuentra tipificada en los modelos normalizados de notificación, dentro del apartado de «*Procedencia y procedimiento de recogida*», únicamente, se podrá señalar este supuesto cuando los datos se hayan obtenido de acuerdo a lo previsto en el artículo 31.1 de la Ley Orgánica 15/1999 que dispone que «*Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral».*

A su vez, la disposición transitoria segunda establece que *«reglamentariamente se desarrollarán los procedimientos de formación del Censo Promocional».* Dado que hasta la fecha no ha sido aprobado el reglamento no puede existir ningún fichero procedente del censo promocional, por lo que, entendiendo que se cometió un error al consignar este supuesto en la declaración, se procedió a subsanar el error material, anulando *«Censo Promocional»* como origen de los datos, en virtud de las competencias atribuidas en el artículo 26.c) del EAPD, en el que se establece que *«El Registro General de Protección de Datos podrá rectificar de oficio los errores materiales de los asientos».* Esta circunstancia fue notificada oportunamente a los responsables de los ficheros, para que en el caso de que no estuvieran de acuerdo con la subsanación realizada presentarán en el plazo de 10 días las alegaciones que considerasen oportunas.

3.2. Ficheros con datos especialmente protegidos de ideología, afiliación sindical, creencias y religión

Durante 2002 se han inscrito 1.822 ficheros de titularidad privada en los que se han declarado datos de carácter personal especialmente protegidos de ideología, creencias, religión

o afiliación sindical, representando un incremento de, aproximadamente, el 150% respecto de los tratamientos con este tipo de datos notificados durante 2001.

Este incremento se justifica en la medida en que una parte muy significativa de los tratamientos inscritos durante 2002 declaran finalidades relacionadas, por una parte, con la gestión de recursos humanos, dentro de las cuales se incluye la gestión del pago de la cuota sindical y, por otra, con las finalidades de gestión contable y administrativa para el trámite de la declaración del IRPF, en las que se declaran datos especialmente protegidos de religión o creencias.

En 1.482 notificaciones se ha declarado que se tratan datos especialmente protegidos de afiliación sindical con la finalidad, en su mayor parte, de hacer efectivo el pago de la cuota a la organización sindical correspondiente, de conformidad con lo previsto en la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical.

En algún caso el responsable ha cumplimentado también este tipo de dato con la finalidad de gestionar el abono de la prima de producción a los trabajadores para lo que es necesario comprobar la prestación real y efectiva del tiempo de trabajo. En el caso de los trabajadores que fuesen miembros del Comité de Empresa, de Centrales Sindicales o Delegados Sindicales electos, era necesario tratar este tipo de datos para determinar, a su vez, la existencia de permisos abonables disfrutados en el ejercicio de sus funciones, en aplicación de la citada Ley Orgánica y del Estatuto de los Trabajadores.

Por lo que respecta a los datos especialmente protegidos de religión se han inscrito un total de 465 tratamientos que notificaban este tipo de datos, de los cuales, la mayoría están relacionados con la confección de autoliquidaciones del IRPF y los donativos, donaciones y aportaciones a determinadas instituciones.

En 96 ocasiones se han declarado tratamientos de datos relativos a creencias e ideología sin consentimiento expreso, relacionados con el ejercicio de profesiones jurídicas, cuya habilitación se encuentra en el derecho a la tutela judicial efectiva reconocido en el artículo 24 de la CE.

Se han inscrito 33 ficheros en cuya notificación figura que se tratan datos especialmente protegidos de afiliación sindical, religión o ideología amparados en la excepción prevista en el segundo inciso del artículo 7.2 de la LOPD, 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 precisa-*

rá siempre el previo consentimiento del afectado». Estos ficheros han sido declarados por partidos políticos, organizaciones sindicales y congregaciones religiosas.

3.3. Ficheros con datos especialmente protegidos de salud, origen racial y vida sexual

Por lo que respecta a los datos especialmente protegidos a que hace referencia el apartado 3 del artículo 7 de la LOPD (origen racial, salud y vida sexual), durante 2002 se han inscrito 22.258 ficheros que han declarado este tipo de datos, frente a los 5.859 que se inscribieron durante 2001. Estas inscripciones han representado un incremento de casi el 280%.

En prácticamente la totalidad de estos ficheros se han declarado datos especialmente protegidos de salud (22.243), la mayor parte relacionados con las inscripciones de las oficinas de farmacia, y en menor medida con entidades de asistencia sanitaria.

En 316 inscripciones se han declarado datos especialmente protegidos de vida sexual relacionados con la asistencia sanitaria, con la finalidad de mantener el historial clínico.

Los ficheros en los que se ha declarado que se tratan datos relativos al origen racial o étnico han sido 153, relacionados con las historias clínicas, ensayos clínicos, reproducción asistida y asistencia social, entre otras finalidades compatibles con la recogida de este tipo de dato.

3.4. Modificación y supresión de inscripciones

Durante 2002 se han realizado un total de 5.336 operaciones de modificación y 4.013 operaciones de supresión en los ficheros de titularidad privada que figuraban inscritos, todas ellas realizadas a solicitud del responsable.

Las modificaciones y supresiones notificadas por los responsables han estado relacionadas con cambios en los sistemas de información, cese de la finalidad para la que fueron creados los ficheros, sustitución de las inscripciones por nuevas inscripciones, cese de actividad y cambios en la titularidad del responsable.

Para notificar estas variaciones, los responsables han podido optar, o bien por modificar las inscripciones existentes, o bien por suprimir las inscripciones antiguas y notificar nuevas inscripciones. En este sentido, cabe señalar, que los responsables pueden optar por un procedimiento u otro, ya que no existe una reglamentación específica que regule estos aspectos del trámite de la notificación de modificaciones, como ya se ha señalado en memorias de años anteriores.

Por lo que se refiere a los cambios en la titularidad del responsable, se pueden señalar, por su especialidad y alcance, los que se han producido en compañías de telecomunicaciones, aseguradoras y eléctricas, estas últimas relacionadas con la previsión legal que obliga a la separación de las actividades destinadas a la generación y distribución de energía eléctrica, establecido en la Ley 54/1997, de 27 de diciembre, de Regulación del Sector Eléctrico desarrollada por el Real Decreto 277/2000 de Energía Eléctrica que establece el procedimiento de separación jurídica de las actividades destinadas al suministro de energía eléctrica.

3.5. Responsable establecido fuera del territorio español

La Directiva 95/46/CE, considera que es necesario que todo tratamiento de datos efectuado en la Comunidad respete la legislación de uno de sus Estados miembros. En este sentido, el tratamiento deberá estar sometido a la legislación del Estado miembro donde esté establecido el responsable y si existiera un encargado del tratamiento bajo la autoridad del responsable en otro Estado miembro, el encargado del tratamiento tendrá que cumplir la legislación del Estado miembro donde esté establecido el responsable, de conformidad con el primer inciso de la letra a) del apartado 1 del artículo 4. Sin embargo, ello no es aplicable cuando una empresa haya decidido ejercer su «derecho de establecimiento» en más de un Estado miembro, en cuyo caso se debe aplicar el segundo inciso del artículo anteriormente citado que señala que *«Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho Nacional aplicable»,* en el sentido de que, en ambos incisos, el artículo se refiere a responsables del tratamiento establecidos en el territorio de un Estado miembro.

No obstante, cuando el responsable del tratamiento no está establecido en el territorio de la Unión Europea y recurra, para el tratamiento de datos personales, a medios situados en el territorio de un Estado miembro, salvo que éstos se utilicen solo con fines de tránsito, deberá cumplir con todas las previsiones establecidas en el artículo 4.1.c de la Directiva[1].

Ante estas circunstancias, al responsable del tratamiento se le aplicarán las disposiciones nacionales de conformidad con el artículo 4.1.c) de la Directiva 95/46/CE, y deberá designar un representante establecido en el territorio de dicho Estado miembro. Estas previsiones de la Directiva tienen su paralelismo en el artículo 2.1.c y el último inciso del artículo 5.1 de la LOPD.

---

[1] Según el Documento de trabajo del GT29 relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, un ejemplo típico de medios utilizados exclusivamente para el tránsito son las redes de telecomunicaciones (nodos centrales, cables, etc.) 5035/01/ES/FI/WP 56. http://www.europa.eu.int/comm/privacy.

El apartado a) del artículo 2.1 de la LOPD condiciona el ámbito de aplicación a aquellos tratamientos de datos de carácter personal que se efectúen en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. En este sentido, será necesario diferenciar si el tratamiento es efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento y, en el caso de que el responsable del tratamiento no esté establecido en territorio de la Unión Europea, si utiliza medios situados en territorio español, excepto si los utiliza solo con fines de tránsito.

Cuando el responsable está establecido en la UE y el tratamiento en España se realiza, únicamente, en el marco de una prestación de servicios, en los términos del artículo 12 de la LOPD, se considera que la entidad responsable del fichero no debe figurar inscrita en la Agencia de Protección de Datos, sin perjuicio de que la entidad establecida en España que realiza la prestación de servicios deba cumplir con las medidas de seguridad establecidas en el Reglamento de Medidas de Seguridad.

A su vez, en su apartado c) establece que también será de aplicación la LOPD cuando el responsable no esté establecido en territorio de la Unión Europea y utilice medios (excepto los de tránsito) situados en territorio español. En estos casos, y de conformidad con el último inciso del artículo 5.1, el responsable deberá designar un representante en España.

Durante el año 2002 se han inscrito 3 ficheros, pertenecientes a otros tantos responsables establecidos fuera del territorio español, 2 de ellos en el Reino Unido y el tercero en los Estados Unidos de América, figurando, a finales de 2002, un total de 23 ficheros inscritos pertenecientes a responsables establecidos fuera del territorio español, 20 de los cuales se encuentran en países de la Unión Europea y los tres restantes en Estados Unidos de América (2) y Suiza (1).

En uno de los tratamientos cuyo responsable está establecido en la Unión Europea, se trataba de una sociedad constituida conforme a las leyes del Reino Unido, que dispone de un establecimiento en España, mediante la forma jurídica de sucursal en España, dotado de representación permanente y autonomía de gestión, pero no de personalidad jurídica, a través de la cual la entidad establecida en el Reino Unido lleva a cabo el desarrollo de sus actividades en territorio español.

En la tramitación de la inscripción de la entidad establecida en los Estados Unidos de América, ha sido necesario determinar si los tratamientos se encontraban incluidos en el ámbito de aplicación de la Ley.

En este caso, el responsable del fichero fundamentó que, aunque, efectivamente, la sociedad responsable del fichero, era una entidad estadounidense, se solicitaba su inscripción en la Agencia dado que se estaban utilizando medios situados en España para el tratamiento

de los datos personales, toda vez que los datos se recababan en el sitio web de la filial española que, además, actuaba como representante en España de la entidad responsable, de conformidad con la previsión del último inciso del artículo 5.1 de la Ley.

En la tramitación de la notificación se aportó la documentación acreditativa de la representación y poderes suficientes del responsable 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 establecidos en el artículo 5 de la LOPD, en especial de la identidad del responsable del fichero y del lugar dónde poder ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Los datos del representante en España, deben figurar inscritos con el fin de que los afectados puedan ejercer los derechos anteriormente citados. Para ello, deberán notificar los datos del representante en España en el apartado de *Servicio o Unidad de Oposición, Acceso, Rectificación y Cancelación,* de acuerdo con las instrucciones de cumplimentación anexas al modelo establecido por la Agencia de Protección de Datos (B.O.E. nº 153, de 27 de junio de 2000).

3.6. Oficinas de farmacia

Se hace una referencia singular a este sector debido al aumento que se ha producido en el último año, ya que durante 2002 se han inscrito alrededor de 15.000 tratamientos de oficinas de farmacia, frente a los más de 2.600 ficheros notificados en 2001.

Al final del año 2002, figuran aproximadamente inscritos 20.000 ficheros correspondientes a oficinas de farmacia.

Este incremento se ha producido a raíz de la firma de un protocolo entre la Unión Profesional de los Colegios Profesionales y la Agencia de Protección de Datos, mediante el que se creó un grupo de trabajo con representantes de los Colegios y Consejos, entre los que se encontraba el Consejo General de Colegios Farmacéuticos.

Las finalidades de los tratamientos notificados se refieren a la gestión, tramitación, grabación y control de prescripciones y dispensaciones de medicamentos efectuados por las oficinas de farmacia a los usuarios del sistema público de salud, entre las que se incluyen las anotaciones previstas legalmente en los libros recetario y de estupefacientes.

En estos ficheros se incluyen datos especialmente protegidos de salud, recogidos y tratados según lo dispuesto en la legislación sanitaria aplicable, en concreto en la Ley de 25/1990 del Medicamento, la Ley de 16/1997 de Regulación de los Servicios de la Oficina

de Farmacia y la Ley de 14/1986 General de Sanidad, así como en la normativa específica de cada Comunidad Autónoma.

En este tipo de tratamiento, y para estas finalidades, no es necesario el consentimiento expreso del afectado, ya que está exceptuado por el artículo 8 de la LOPD, en conexión con la legislación en materia de sanidad.

Las cesiones previstas para este tipo de tratamientos tendrían como destinatarios de las mismas a los Colegios Profesionales, Consejo General de los Farmacéuticos y las Administraciones Públicas con competencias en materia farmacéutica.

Además, se han declarado ficheros cuya finalidad es la gestión de los clientes de las oficinas de farmacia. En estos casos, si se incluyeran datos especialmente protegidos de salud, se deberá recabar el consentimiento expreso de los afectados. Finalmente, también en este sector, se han declarado los tratamientos cuya finalidad es la gestión de los recursos humanos de la oficina de farmacia.

3.7. Tratamientos no automatizados

Durante el año 2002 se han notificado para su inscripción 1.748 tratamientos no automatizados, frente a los 326 ficheros de estas características inscritos en el 2001. La mayor parte de estos tratamientos están relacionados con las inscripciones de oficinas de farmacia, citadas anteriormente, en aquellos casos en que el libro recetario oficial no esté informatizado y únicamente se disponga en soporte papel. También en el sector sanitario se ha notificado este tipo de tratamiento con la finalidad de recoger el historial clínico. En menor medida, se han declarado tratamientos manuales con la finalidad de gestionar los expedientes de los clientes de despachos de abogados o, en otros casos, tratamientos relacionados con la vigilancia médica de los empleados.

Estos tratamientos manuales no se incluyen en el ámbito de aplicación del Reglamento de Medidas de Seguridad. Por lo tanto, para notificarlos sin especificar el nivel de seguridad, será necesario, utilizar el modelo normalizado en soporte papel, ya que el programa de ayuda para la notificación de ficheros no permite la declaración de ficheros manuales, toda vez que este soporte únicamente está previsto para declarar ficheros o tratamientos automatizados.

3.8. Dudas que se plantean en la cumplimentación de notificaciones

A modo de resumen, se pueden sintetizar algunas situaciones que han sido objeto de consulta por parte de los responsables de ficheros:

Dudas planteadas acerca de la notificación de ficheros con datos especialmente protegidos

Durante la tramitación de algunos expedientes de inscripción con datos de esta naturaleza y ante la posibilidad de que se hubieran producido ciertos errores al cumplimentar la notificación, se ha requerido a los responsables para que subsanasen el posible error o procedieran a efectuar las alegaciones que estimasen oportunas, al objeto de aclarar las circunstancias en las que se produce el tratamiento de este tipo de dato.

En la mayor parte de los casos, los responsables han subsanado sus declaraciones debido a que, efectivamente, se había producido un error al cumplimentar el apartado de *Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero.* No obstante, en algunos casos, han manifestado, en las alegaciones presentadas, el motivo que les ha llevado a recoger y tratar este tipo de datos.

En este mismo orden, cabe señalar las alegaciones presentadas por una entidad financiera que había considerado pertinente notificar datos de ideología, afiliación sindical, religión y salud en un tratamiento cuya finalidad era tramitar los adeudos por domiciliaciones, de forma separada del tratamiento genérico de clientes.

Esta decisión fue tomada, entre otras razones, porque determinados adeudos por domiciliaciones llevan incorporados datos que podrían considerarse especialmente protegidos, en función de la identidad del emisor (por ejemplo, un sindicato, una asociación de enfermos, un instituto religioso o un partido político) o del concepto que venga indicado en el soporte magnético (cuota de afiliado o de asociado). Pues bien, es criterio de la Agencia que estos tipos de datos especialmente protegidos deben ser incluidos en el subapartado *«Datos especialmente protegidos»* en el apartado «*Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero»* de la notificación del fichero.

En el mismo sentido, aunque en este caso más habitual, se notifican datos de ideología, religión o creencias en tratamientos relacionados con los asuntos tramitados por los asesores fiscales, consignando en las notificaciones estos tipos de datos especialmente protegidos, dentro del marco global del asesoramiento a clientes o confección de declaraciones del Impuesto de la Renta de las Personas físicas.

La Ley de Presupuestos Generales del Estado, establece el sistema de asignación tributaria a la Iglesia Católica. En su virtud, el Estado destina al sostenimiento de la Iglesia Católica el 0.5239 por 100 de la cuota íntegra del Impuesto sobre la Renta de la Personas Físicas correspondiente a los contribuyentes que manifiesten expresamente su voluntad en tal sentido, pudiendo optar, también, por destinar dicho porcentaje a fines sociales (Organiza-

ciones no Gubernamentales de Acción Social y de Cooperación al Desarrollo para la realización de programas sociales).

Si bien, por una parte, resulta evidente que al cumplimentar las declaraciones del IRPF queda reflejada en soportes informáticos la opción sobre el destino de la asignación tributaria, y en este sentido hay opiniones que afirman que, efectivamente, se están tratando datos especialmente protegidos, también hay opiniones en el sentido contrario, es decir que sostienen que resulta excesivo establecer que una opción de asignación tributaria indica las creencias de un determinado individuo. El criterio de la Agencia, al respecto, es que el tratamiento de esta circunstancia y su almacenamiento en un soporte supone un tratamiento de datos especialmente protegidos y los mismos deben ser notificados en el subapartado *«Datos especialmente protegidos».*

Por otra parte, en algunas notificaciones se ponen de manifiesto errores al cumplimentar el apartado de *«Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero / Otros datos especialmente protegidos»,* dado que señalan la casilla correspondiente a *Origen racial o étnico,* cuando, en realidad, se están recabando datos relativos a la nacionalidad.

En otras ocasiones, al tramitar los expedientes de inscripción, se observa que, del contenido de la declaración, se pudiera deducir que el tratamiento declarado debiera incluir datos especialmente protegidos que no se han consignado en la notificación. Ante esta situación, y ante la posibilidad de que se hubiese cometido un error, se requiere al responsable del tratamiento para que subsane o realice las alegaciones que estime pertinentes.

Dentro de este caso se encuentran las declaraciones en las que se había señalado en el *Apartado de Responsable del fichero o tratamiento,* como código de actividad principal de la entidad responsable del fichero, *«Actividades políticas, sindicales y religiosas»* y, sin embargo, no se había señalado que se recabaran datos especialmente protegidos relacionados con sus miembros o socios.

Con el fin de advertir del posible error, se informó al responsable de que el código de actividad tipificado como *«Actividades políticas, sindicales y religiosas»,* únicamente debía ser señalado cuando los asociados o miembros pertenezcan a un partido político, sindicato, entidad religiosa o una asociación o fundación cuyos fines sean políticos, sindicales o religiosos. Para los casos en los que el responsable no estuviera incluido en este tipo de actividad existía un código de actividad principal, tipificado como *«Actividades asociativas diversas».*

No obstante, si la entidad responsable del fichero estuviera constituida como una asociación, y los estatutos de dicha asociación establecieran la necesidad de que sus miembros o asociados pertenecieran a una determinada religión o ideología, se entiende que ese trata-

miento sí podría revelar la ideología, creencias o religión y, por lo tanto, será necesario que se cumplimente el apartado de *«Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero / Datos especialmente protegidos».*

Otras situaciones en las que se producen dudas, en relación con los datos especialmente protegidos, son las referentes a los casos en los que se tienen previsto realizar transferencias internacionales a entidades establecidas en países que no ofrecían un nivel de protección adecuado. En ellas se ha exigido que en la cláusula, mediante la que se solicitaba el consentimiento inequívoco a la transferencia, se incluya el consentimiento expreso exigido en el tratamiento de datos especialmente protegidos, de conformidad con el artículo 7 de la LOPD, de manera que dicho consentimiento incluyera una mención expresa de que se tenía previsto transferir este tipo de datos.

Dudas sobre la cumplimentación del apartado de «Responsable del fichero o tratamiento»

Se ha planteado, con bastante frecuencia a la hora de cumplimentar el modelo de notificación, una duda que ha consistido en que el solicitante cumplimenta el apartado de *Responsable del fichero* con los datos correspondientes al empleado o directivo que tiene la responsabilidad funcional del área relacionada con los datos y finalidades que se incluyen en el fichero.

Los criterios que se deberán tener en cuenta para determinar la identidad del responsable del fichero, son los que establece la LOPD, en el apartado d) del artículo 3 en el que se considera responsable del fichero o tratamiento *«la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del fichero o tratamiento».*

Así mismo, el artículo 5 de la citada Ley, que regula el derecho de información en la recogida de datos, establece que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco, entre otros extremos, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

A su vez, podrán crearse ficheros de titularidad privada, que contengan datos de carácter personal, cuando resulten necesarios para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular, de conformidad con lo establecido en el artículo 25 de la Ley 15/1999.

Por lo tanto, para determinar la identidad del responsable del fichero se deberá tener en cuenta lo establecido en los artículos 3 d), 5.1 y 25 de la LOPD. En todo caso, los datos identifica-

tivos que figuran en la cláusula, mediante la que se cumple con el derecho de información en la recogida de los datos a que se refiere el citado artículo 5, serán los que deban figurar, a los efectos de inscripción en el RGPD, en el apartado de *Responsable del fichero o tratamiento.*

En otras ocasiones, han surgido dudas al figurar como responsable del fichero entidades, servicios o centros de servicios sociales, cuya actividad correspondía a una asociación de interés social.

Durante la tramitación de estos expedientes se ha tratado de clarificar si estas entidades eran responsables del tratamiento o si estaban realizando una prestación de servicios por cuenta de organismos públicos con competencias en materia de servicios sociales dentro de los servicios sociales especializados, como, por ejemplo, la atención social a las personas mayores, a los discapacitados, a los drogodependientes, a las personas con riesgo o situación de exclusión social, etc.

Aunque la normativa dictada por las Comunidades Autónomas en materia de servicios sociales es muy amplia, estas normas reglamentan y establecen los criterios que deben cumplir las entidades, servicios y centros públicos y privados, con o sin ánimo de lucro, que presten servicios sociales.

Si bien la responsabilidad pública de promover y garantizar la prestación de servicios sociales recae sobre los órganos competentes de la Comunidades Autónomas, no obstante las entidades que prestan estos servicios podrían ser responsables de los tratamientos que fueran necesarios para gestionar los mismos.

Dudas sobre la cumplimentación de la «Hoja de solicitud»

Cuando el responsable del fichero notifica una inscripción al RGPD, debe hacer constar los datos relativos a la persona física que actúa como declarante y la dirección a efectos de notificación, en la *hoja de solicitud* que forma parte del modelo de notificación.

En determinadas ocasiones si la persona que en su día firmó la solicitud ha cesado en su cargo, se solicita la modificación de los datos que figuran inscritos para que consten los datos identificativos de la persona que tiene la representación de la entidad en la actualidad.

Es necesario tener en cuenta que los datos relativos a la persona física que actúa como declarante de la notificación no forman parte registral de la inscripción del fichero. Sus datos identificativos únicamente se tratan a los efectos previstos en los procedimientos administrativos que sean necesarios para la tramitación de las correspondientes inscripciones de las notificaciones presentadas, por lo que no procede notificar este tipo de cambio.

Dudas acerca de si cualquier tratamiento de datos en el que esté involucrada una entidad o persona establecida fuera del territorio español es una transferencia internacional de datos

En algunos tratamientos de datos relacionados con la gestión de la cartera de clientes que tienen su domicilio fuera del territorio español, el responsable del fichero ha entendido que realizaba una transferencia internacional de datos, puesto que emite las facturas a la dirección del cliente, y ésta se encuentra fuera del territorio español.

En un principio, cabe entender que no se está produciendo una transferencia internacional ni tampoco una cesión de datos, puesto que por tal se considera toda revelación de datos a un tercero distinto del afectado o el responsable, por lo que, en este caso, la comunicación de los datos al propio afectado no constituye una cesión de datos.

No obstante, lo señalado en el párrafo anterior, sí se producen flujos internacionales de datos en las transferencias bancarias para la gestión de cobros y pagos de clientes cuyo domicilio se encuentra fuera del territorio español. En estos casos, son las entidades financieras, a las que las leyes reconocen como prestadoras servicios bancarios, las que realizan estas transferencias y, por lo tanto, deberán constar en los ficheros de su titularidad estas transferencias internacionales. A tal fin, se señalará, en el apartado de *Transferencias internacionales,* como destinatarios de las transferencias las *«Entidades financieras internacionales (bancos y cajas para ejecución de cobros y pagos)»,* amparadas en lo dispuesto en el apartado d) del artículo 34 de la LOPD que exceptúa de la norma general las transferencias dinerarias realizadas conforme a su legislación específica.

Dudas acerca de la cumplimentación del apartado «Encargado de tratamiento»

En el apartado de *Encargado del tratamiento* es preciso resaltar dos situaciones. Una de ellas, se produce en aquellos casos en los que se quiere notificar la existencia de más de un encargado, ya que el modelo de notificación únicamente contempla la posibilidad de notificar un solo encargado. La segunda, se produce cuando no se puede distinguir si se trata de una prestación de servicios, en los términos previstos en el artículo 12 de la Ley o de una cesión de datos.

En primer lugar, es necesario tener en cuenta que el apartado de *Encargado de tratamiento* no es de notificación obligatoria, por lo que, a los efectos de inscripción, no es necesario cumplimentar todos los encargados que traten datos de carácter personal por cuenta del responsable. Con carácter general, se ha informado a los responsables que, si bien este tratamiento por cuenta de terceros deberá estar regulado en un contrato que deberá constar por escrito en los términos del artículo 12 de la Ley, a los efectos de inscripción, única-

mente se consignarán en dicho apartado los datos de uno de los encargados del tratamiento. Se recomienda que se haga constar la denominación del encargado que realice el tratamiento de datos que pueda implicar una mayor duración en el tiempo, o riesgos mayores según el tipo y la cantidad de datos tratados.

No obstante, en alguna ocasión, se ha puesto de manifiesto que se notificaban distintas finalidades (clientes, recursos humanos, gestión bancaria, etc.) en una misma declaración, y que el responsable pretendía con una única declaración notificar conjuntamente los encargados de tratamiento correspondientes a todas estas finalidades. En estos casos, se debe realizar una notificación por cada uno de los distintos tratamientos o usos del fichero, teniendo en cuenta la diversidad de colectivos de afectados, de esta manera se pueden incluir en cada notificación los datos de un prestador de servicios.

También hay que mencionar los casos en los que se pretende cumplimentar el apartado de *Encargado del tratamiento,* haciendo constar las denominaciones de las entidades que, en realidad, son destinatarios de cesiones de datos, en vez de prestadores de servicios por cuenta del responsable del fichero.

En este sentido, es necesario determinar si la transmisión de datos constituye una cesión de datos o si, por el contrario, dicha transmisión supone la realización de un tratamiento por cuenta del responsable del fichero, de acuerdo con las previsiones del artículo 12 de la Ley.

En el caso de que los datos se destinen, no para la simple realización de actividades de tratamiento por cuenta del responsable (artículo 12 de la Ley), sino para incorporar la información a los ficheros de la entidad destinataria, su transmisión será constitutiva de una cesión de los mismos, de conformidad con el artículo 3 i) de la LOPD, cuando la define como *«toda revelación de datos realizada a una persona distinta del interesado».*

En este caso de cesión, se deberá cumplimentar el apartado de *Cesión o comunicación de datos,* indicando los destinatarios de las mismas o, en el caso de que exista un número indeterminado de ellos, las reglas que permitan su identificación, de acuerdo con las instrucciones del modelo de notificación, y no se deberá cumplimentar en el apartado de *Encargado del tratamiento.*

Dudas relacionadas con la cumplimentación del apartado «Procedencia y procedimiento de recogida de los datos»

Por su relevancia merecen ser señalados los tratamientos relacionados con los datos de carácter personal de menores de edad. Como ejemplo, se puede citar la situación que se produce cuando los familiares para hacer un regalo (abuelos, tíos, etc.) contratan con empresas

que se dedican a esta actividad, incluyendo una foto del menor para su publicación en Internet. El responsable del fichero había notificado que los datos procedían de *«Otras personas distintas del interesado o su representante legal»*, sin embargo, se informó al responsable de que, en tales supuestos, es preceptivo, antes de publicar en Internet la foto y los datos de un menor de edad, que se recabe el consentimiento de los representantes legales del menor.

4. Inscripción de Ficheros de Titularidad Pública

4.1. Evolución en la inscripción de ficheros de titularidad pública

En el año 2002 se han realizado 7.030 asientos registrales, con base en las solicitudes presentadas por responsables de ficheros de titularidad pública de las diferentes Administraciones Públicas. De estas operaciones, 4.625 han correspondido a inscripciones de nuevos ficheros, 1.876 a modificaciones y 529 a supresiones de inscripciones previas.

Este número de operaciones efectuadas en 2002 ha supuesto un incremento superior al 80% respecto de las solicitudes de inscripción notificadas en el año anterior, concentrándose este aumento en un crecimiento del 287% en la inscripción de nuevos ficheros y un 26% en la modificación de inscripciones, manteniéndose la proporción de años anteriores en el número de supresiones.

Al responder estas notificaciones al propósito de adecuar las inscripciones de ficheros a la LOPD, se puede observar que de las 1.876 operaciones de modificación realizadas, 748 (40%) contenían modificaciones en el apartado de *Cesiones de datos* y 237 (13%) en el apartado *Medidas de seguridad,* lo que se relaciona directamente con la aplicación de la STC 292/2000 y el Reglamento de Seguridad.

Por otra parte, también se han realizado 1.111 operaciones de oficio, lo que ha supuesto un incremento del 66% en relación con el año anterior. Su objetivo ha sido la adecuación de los formularios de notificación a los criterios de normalización de las inscripciones. Generalmente, estas operaciones se producen en el apartado del *Responsable,* sin embargo, este año 522 han correspondido al apartado *Cesiones de datos* y 30 al de *Medidas de seguridad* cuando se había consignado en la notificación un nivel que no coincidía con el nivel publicado en la disposición.

Al finalizar el año, figuran inscritos en el RGPD 35.894 ficheros de titularidad pública, lo que ha supuesto un crecimiento superior al 12% respecto a las cifras correspondien-

tes a 2001, y ha quintuplicado el número de inscripciones que se venía realizando en los últimos años.

No obstante, la notificación del apartado *Medidas de seguridad* no ha alcanzado las expectativas que se habían previsto como consecuencia del fin del plazo establecido por el Reglamento de Seguridad. Sin embargo, dado que la adecuación de cada disposición a la LOPD también implica la publicación del nivel de medidas de seguridad exigibles a cada fichero, es previsible que la notificación de este apartado se produzca una vez haya sido publicada la modificación de la norma habilitante.

De los 4.625 nuevos ficheros de titularidad pública inscritos al finalizar el año, 144 corresponden a la Administración General del Estado, que durante 2002 ha incrementado en un 65,52% el número de inscripciones de 2001.

El mayor número de inscripciones se ha concentrado en las Administraciones de las Comunidades Autónomas con 3.859 notificaciones. Este aumento se ha debido a la notificación de los ficheros de colegios e institutos de enseñanza, competencia transferida a la Comunidad de Madrid, que ha optado por notificar individualmente los ficheros de cada uno de los centros docentes.

Las Entidades Locales han notificado 610 nuevos ficheros, un 50% más que el año anterior. Si bien no constan inscritos la totalidad de ayuntamientos existentes, se puede afirmar que los que figuran inscritos encuadran casi al 92% de la población. En el cuadro siguiente puede comprobarse la distribución de los Ayuntamientos que aún no han inscrito sus ficheros por tramos de población.

Tramos población (nº habitantes)	Ayuntamientos	Habitantes[2]/ Tramo	Avuntamientos inscritos	% Población/ Aytos. inscritos
< 1.000	4.898	1.638.041	1.342	35,61
1.000 - 4.000	1.885	3.838.602	1.026	55,11
4.001 - 7.500	540	2.974.474	519	96,10
>7.500	764	31.339.838	753	98,74
TOTAL	**8.087**	**39.790.955**	**3.640**	**91,73**

Del análisis de la evolución de la inscripción de ficheros de titularidad pública, se puede concluir que el aumento del número de inscripciones realizado durante este año se ha debido a la forma de notificar los diferentes sistemas de información, no tanto a que no se encontrasen debidamente inscritos anteriormente, salvo las notificaciones relativas a

[2] Datos publicados por el INE a 1-1-2002.

los nuevos tratamientos que se ponen en marcha sucesivamente en las diferentes administraciones.

El aumento global del número de operaciones realizadas en el RGPD sobre ficheros de titularidad pública ha ascendido hasta un 80%, correspondiendo con las notificaciones de adecuación de la inscripción, relacionadas con los tres hechos ya citados, que tenían repercusión durante este año: STC 292/2000, Reglamento de Seguridad y Disposición Adicional.

Sin embargo, la forma de realizar esta actualización se ha efectuado de acuerdo a diversos criterios de los órganos titulares de los ficheros y tratamientos. Así, en ocasiones han dado lugar a operaciones de modificación de las inscripciones iniciales, mientras que en otros casos se han reorganizado los sistemas de información, notificando nuevos ficheros ya adecuados a la nueva normativa y suprimiendo las inscripciones anteriores. Lo que justifica en cualquier caso, el aumento del número de operaciones registradas durante los últimos meses.

Para evitar estas actuaciones opcionales sería necesario que estuviera desarrollado reglamentariamente un procedimiento único de notificación de las inscripciones al RGPD.

Para el próximo ejercicio es previsible que se mantenga una magnitud de inscripciones similar a la de este año, dado que se continuarán publicando las disposiciones de adecuación de ficheros, que darán lugar a las posteriores notificaciones de conformidad con el art. 20 de la LOPD y los artículos 5 y 7 del Real Decreto 1332/1994.

Por otra parte, también se puede prever que las transferencias de competencias, que se han producido durante los últimos años en materia de educación y de gestión hospitalaria de la Administración General del Estado a las Comunidades Autónomas, supondrán cambios en la titularidad de los ficheros, y tendrán su reflejo en el RGPD, al menos, en las correspondientes actualizaciones de denominaciones de los órganos titulares con responsabilidad sobre los mismos.

Así mismo, las transferencias de competencias pueden dar lugar a reorganizaciones de los sistemas de información, que junto con la necesidad de adecuación de las disposiciones de creación de ficheros, podrían producir un elevado número de actualizaciones en el futuro.

También, se podrían producir nuevas inscripciones de ficheros de titularidad pública durante el año 2003 y siguientes, si como es previsible los convenios de colaboración de la Agencia con los colectivos de Notarios, Registradores, Colegios Profesionales y Cámaras de Comercio comienzan a producir sus frutos y se publican en los distintos boletines oficiales las órdenes reguladoras de los ficheros que son responsabilidad de estas instituciones. En este sentido, al cierre de esta memoria, ya ha sido publicada la disposición general de creación de los ficheros de Notarios, Colegios Notariales y Consejo General del Notariado, y se encuentra muy avanzada la tramitación de la correspondiente a Registradores.

4.2. Repercusión de la STC/292/2000 y el Reglamento de Seguridad en la inscripción de ficheros de titularidad pública

Con fecha 4 de enero de 2001, se publicó en el BOE la sentencia 292 del Tribunal Constitucional de 30 de noviembre, dictada en relación con el recurso de inconstitucionalidad 1463/200 promovido por el Defensor del Pueblo respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999.

A tenor de lo dispuesto en el art. 21.1 de la LOPD, las Administraciones Públicas estaban habilitadas para realizar la cesión de datos siempre que hubiere sido prevista tal cesión en la propia disposición de creación del fichero, rebajando el rango de la norma que autorizaba la cesión.

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»* 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 legítimas del cedente y del cesionario con el previo consentimiento del interesado»*, aún cuando, tal como determina el apartado 2 del mismo artículo no será preciso dicho consentimiento, entre otros casos, *«cuando la cesión está autorizada por una Ley»*.

Por otra parte, para el ámbito exclusivo de las cesiones de datos entre Administraciones Públicas el art. 21, en la redacción resultante de la publicación de la STC 292/2000 dispone que:

> *«1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*
> *2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.*
> *3. No obstante lo establecido en el artículo 11.2 b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.*
> *4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.»*

Por tanto, cualquier cesión de datos entre Administraciones Públicas sólo podrá efectuarse si se cumplen algunas de las previsiones anteriormente citadas.

Como a partir de la STC/292/2000 no era posible realizar una cesión, por el mero hecho de ampararse en la norma de creación de ficheros, desde la citada publicación se ha venido informando del fallo de la misma a los 119 responsables de ficheros que figuraban con inscripciones en las que se declaraba la posibilidad de realizar cesiones en los términos que la sentencia había anulado, es decir, amparándose únicamente en el hecho de que la orden de creación del fichero hubiera habilitado esa posibilidad.

Al finalizar 2002, el número de notificaciones recibidas para adecuar la declaración del apartado *Cesiones* a lo señalado en la citada Sentencia, ha alcanzado al 45% de los que constaban inscritos en los términos anteriormente planteados.

Los ficheros que aún se encuentran inscritos de acuerdo la declaración inicial, en la que se hacía constar la realización de cesiones de datos amparándose únicamente en la norma de creación del fichero, deberán adecuarse en el aspecto formal notificando las variaciones que correspondan del apartado de *Cesiones.* No obstante, al igual que ocurre con la adecuación del apartado *Medidas de seguridad* es de esperar que aprovechando la necesidad de adaptar la norma de creación del fichero a la LOPD se analicen las circunstancias en las que tienen lugar las distintas cesiones de datos adecuándolas a los supuestos legales en que éstas pueden realizarse.

El vencimiento en 2002 del último de los plazos establecidos en el Reglamento de Seguridad para la aplicación de las medidas de seguridad correspondientes al nivel alto, como ya se ha señalado anteriormente, se ha unido con la necesidad de adecuación de la correspondiente disposición a la LOPD.

Esta adaptación exige que se publique en el diario oficial correspondiente una disposición que contemple el nivel de seguridad que deben tener implantados los tratamientos y ficheros de los que son titulares las Administraciones Públicas y otras entidades públicas, previsión que no contemplaba la derogada LORTAD.

4.3. Adecuación a la Disposición Adicional Primera de la LOPD

Como ya se ha expuesto anteriormente, la disposición adicional primera de la LOPD establecía un plazo de 3 años desde su entrada en vigor para adecuar los ficheros y tratamientos automatizados en el Registro General de Protección de Datos a esta Ley. En este plazo, que concluye el 14 de enero de 2003, las Administraciones Públicas responsables de ficheros deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

Por otra parte, con la entrada en vigor de la LOPD, también deben publicarse las correspondientes disposiciones generales de regulación de los Registros Públicos que contengan datos de carácter personal, dado que estos ficheros, que, con la derogada LORTAD, se encontraban exceptuados de su ámbito de aplicación, están ahora sometidos a las disposiciones de la Ley.

Dado que este plazo ha finalizado 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 han comenzado a preparar estas normas durante 2002.

En muchas ocasiones, como ya hemos indicado, los órganos titulares han aprovechado este proceso de adecuación para revisar la situación de sus ficheros en relación con las cesiones de datos, en aplicación de la STC 292/2000, y las adecuaciones a las nuevas estructuras orgánicas departamentales.

En este sentido, al finalizar 2002, los Ministerios de Economía, Fomento, Hacienda, Ciencia y Tecnología, Educación, Cultura y Deporte, y la Dirección General de la Policía ya han publicado nuevas Órdenes Ministeriales de adecuación a la LOPD. También han iniciado la adaptación de las normas habilitantes de regulación de sus ficheros las Comunidades Autónomas de: Andalucía, Castilla La Mancha, Galicia, Madrid, Navarra, La Rioja y Valenciana. En el ámbito de la Administración Local se ha comenzado la elaboración de estas órdenes, si bien, se observa la concentración por provincias, como Zaragoza o Valencia, en donde se han coordinado todos los trámites en una dependencia que es la que formalmente ha procedido a realizar los trámites necesarios para adecuar sus ficheros y tratamientos a las previsiones de la LOPD.

En la elaboración de estas disposiciones se han revisado los sistemas de información existentes en cada departamento, por lo que no sólo se han publicado los aspectos relativos a cada uno de los ficheros existentes, exigidos por la LOPD y que no estaban contemplados en la LORTAD, sino todos aquellos que habían sido modificados desde la publicación inicial de los ficheros. Así mismo, se han publicado disposiciones de ficheros de nueva creación, y en su caso, las supresiones de ficheros que ya no estaban siendo utilizados, bien por haberse incorporado a nuevos ficheros, bien por haber dejado de ser necesarios para los fines en virtud de los cuales se crearon.

La publicación de la disposición que habilita a crear ficheros, no es suficiente para completar el trámite exigido por la Ley. Una vez publicada la disposición en el boletín oficial que corresponda, el órgano titular está obligado a notificar el fichero para su inscripción en el RGPD, de conformidad con los artículos 5 y 7 del Real Decreto 1332/1994. No obstante, algunas unidades han procedido diligentemente a ello, como la Dirección General de la Policía, que en el mes de septiembre ya había notificado y por lo tanto figuraba actualizada su inscripción, como puede comprobarse en el Catálogo de ficheros publicado en la página web de la Agencia.

4.4. Comunidades Autónomas con competencias en materia de protección de datos

Con fecha 14 de mayo de 2002, se publicó en el BOE, la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos. Se une la previsión de esta autoridad autonómica a la de la Comunidad de Madrid, regulada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, que derogaba la Ley 13/1995, de 21 de abril, de regulación del uso de informática en el tratamiento de datos personales por la Comunidad de Madrid, en vigor hasta entonces.

La Ley Catalana crea el Registro de Protección de Datos de Cataluña, aunque al cierre de esta Memoria no se ha establecido el procedimiento de inscripción previsto en el art. 15.3, que aún queda pendiente de su desarrollo reglamentario.

No obstante, la posibilidad de creación de Registros autonómicos, establecida en el artículo 41.2 de la LOPD en el que se establece que *«Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos»,* no condiciona la función esencial, que la LOPD atribuye al RGPD[3], derivada de lo exigido por la Directiva 95/46/CE, de dar publicidad a los tratamientos de datos de carácter personal realizados en todo el territorio del Estado español, esto es, atribuye al RGPD el cumplimiento de la finalidad que motiva su propia existencia a tenor de la Directiva Comunitaria.

Por lo tanto, y en virtud de lo dispuesto en el artículo 14 de la LOPD, relativo al *Derecho de Consulta al Registro General de Protección de Datos «Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita».*

El art. 24 del EAPD impone la inscripción en el RGPD de los ficheros que sean de titularidad de cualesquiera Administraciones Públicas, sin diferenciar entre los correspondientes a la Administración autonómica o local de aquellas Comunidades Autónomas que constituyan, con arreglo a lo establecido en el art. 41 de la LOPD sus propias autoridades de control, regulando en los artículos 5 y siguientes del Real Decreto 1332/1994 los requisitos y procedimientos para proceder a la notificación y ulterior inscripción de los tratamientos en el RGPD.

---

[3] Ver apartado de esta Memoria, Aspectos Internacionales de la Protección de Datos: Análisis de las Tendencias Legislativas, Jurisprudenciales y Doctrinales en relación con el RGPD.

Por lo tanto, en cumplimiento de la LOPD, independientemente de la ubicación territorial de los responsables, todos los ficheros y tratamientos de titularidad pública tienen que figurar inscritos en el RGPD, independientemente de las competencias que la legislación autonómica otorgue a los registros administrativos que se puedan crear en las autoridades de control autonómicas.

No obstante, tal como ya viene sucediendo con la Agencia de Protección de Datos de la Comunidad de Madrid, desde el RGPD se mantienen mecanismos de colaboración y cooperación a fin de facilitar la inscripción de los tratamientos, tanto en sus registros autonómicos como en el RGPD.

Durante 2002, la Agencia de Madrid ha comunicado las notificaciones correspondientes a los responsables de titularidad pública de su ámbito de aplicación, y como ya se ha mencionado en esta Memoria, ha tenido especial relevancia el número de operaciones de inscripción generadas en relación con los ficheros correspondientes a colegios y centros de enseñanza dependientes de esta Comunidad a partir de la transferencia de competencias recibidas del Estado, que han supuesto un número de 1.265 nuevas inscripciones de ficheros de centros de enseñanza.

Circunstancias como éstas, dificultan las comparaciones estadísticas de los datos de inscripciones por Comunidades Autónomas. En este sentido, hay que tener en consideración que otras Comunidades Autónomas tienen declarados entre 2 y 6 ficheros para la finalidad de gestión de sus centros de enseñanza y colegios no habiendo optado por la realización de notificaciones individuales por cada centro o colegio.

Los responsables de ficheros correspondientes a la gestión de centros docentes han optado por notificar un fichero marco de alumnos, en algunos casos diferenciando cada nivel de enseñanza, dependiendo de la consejería o departamento que detenta la competencia, indicando como unidad o servicio de acceso, o bien, el de los servicios centrales que se identifican como responsable del fichero, o bien, el de cada centro docente, con carácter general, sin especificar cada una de las direcciones.

4.5. Implicación del traspaso de competencias a las CCAA en la inscripción de ficheros

El traspaso de competencias de la Administración General del Estado a las diferentes Comunidades Autónomas conlleva el traspaso de las funciones, servicios y medios, entre los que se encuentran los ficheros de datos de carácter personal adscritos a los mismos. Ésto supone, a efectos de inscripción en el RGPD, una modificación del órgano titular responsable de los ficheros.

De no efectuarse esta modificación, la información del RGPD se desactualiza, y no permite facilitar una información veraz sobre la existencia de ficheros inscritos en el Registro, para que el ciudadano pueda ejercitar los derechos que la Ley le reconoce en la protección de sus datos personales.

Por una parte, el art. 20 de la LOPD establece que la creación, modificación o supresión de ficheros de las Administraciones Públicas sólo puede realizarse mediante una disposición general. A los efectos de su inscripción, el cambio de titularidad de los ficheros objeto de un traspaso de competencias puede llevarse a cabo mediante la supresión de los ficheros por parte de la Administración que realiza el traspaso y la creación de nuevos ficheros por parte del órgano que los recibe, o bien mediante la modificación de la denominación del órgano responsable de cada fichero.

En cualquier caso, el art. 5 del Real Decreto 1332/1994 establece que el órgano competente de la Administración responsable del fichero debe notificar a la Agencia los ficheros correspondientes. Así mismo, el art. 8 también establece que deberá darse traslado a la APD de una copia de la disposición general que modifique o suprima los mismos.

En este sentido, la Agencia considera que los Reales Decretos de transferencias se podrían presumir como la disposición general de modificación de la titularidad del órgano responsable que figure inscrito hasta la fecha de la transferencia.

No obstante, a continuación se exponen las distintas situaciones que se han producido con las transferencias en materia de sanidad y educación. Se comentan estos dos casos por afectar a un colectivo importante, tanto de ficheros como de población afectada, aunque se trata de una problemática que se produce con cierta frecuencia con cada uno de los traspasos que se realizan entre administraciones.

El día 1 de enero de 2002, las últimas Comunidades Autónomas que conformaban el denominado territorio INSALUD, asumieron las competencias sanitarias que hasta entonces había ejercido el Estado, a través del Ministerio de Sanidad y Consumo.

En diciembre de 2001 se publicaron los Reales Decretos 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478 y 1479, de 27 diciembre, sobre traspaso de las funciones y servicios del Instituto Nacional de Salud a las Comunidades Autónomas del Principado de Asturias, Cantabria, La Rioja, Región de Murcia, Aragón, Castilla y León, Castilla-La Mancha, Illes Balears y Madrid. El artículo 1 de estos Reales Decretos establece que *«se traspasan a la Comunidad... las funciones y servicios del Instituto Nacional de la Salud»* y el artículo 2 establece que *«quedan traspasados a la Comunidad... las funciones y servicios, así como los bienes, derechos y obligaciones, el personal y los créditos presupuestarios adscritos a los mismos».*

Estos Reales Decretos han implicado un cambio en la titularidad de los ficheros de datos de carácter personal de los centros públicos sanitarios ubicados en las comunidades autónomas afectadas por el traspaso, al encontrarse éstos entre los bienes traspasados.

Al no haber comunicado las CCAA receptoras de las competencias estas modificaciones al RGPD, la Agencia ha informado al respecto al Ministerio de Sanidad y Consumo. Sin embargo, a 31 de diciembre de 2002, estos ficheros siguen figurando bajo la dependencia del Ministerio. Si persiste esta situación la APD procederá de oficio a modificar las inscripciones de estos ficheros de conformidad con los Reales Decretos de transferencias.

Otra transferencia de competencias que ha supuesto modificaciones importantes, a los efectos registrales, es la correspondiente al desarrollo legislativo y ejecución de la enseñanza en toda su extensión, niveles y grados, modalidades y especialidades.

Aunque ya algunas Comunidades la habían asumido con anterioridad, fue en el año 2000, cuando las Comunidades de Madrid, Murcia, Castilla y León, Extremadura, Castilla La Mancha y Asturias recibieron, respectivamente, el traspaso en materia de educación no universitaria, mediante sendos Reales Decretos 926, 938, 1340, 1801, 1844 y 2081 de 1999.

Estos Reales Decretos culminan el proceso de traspasos competenciales en materia de educación no universitaria a la totalidad de las Comunidades Autónomas, a excepción de las ciudades autónomas de Ceuta y Melilla, y así queda reflejado en los artículos 1 y 2 de los citados Reales Decretos, en los que se especifica que *«Se traspasan funciones y servicios de la Administración del Estado en materia de enseñanzas no universitarias a la Comunidad ...»* (art. 1) y en consecuencia según el artículo 2 *«Quedan traspasadas a la Comunidad ... las funciones y servicios a que se refiere...».*

En estos casos, también cabe entender que de los Reales Decretos se deducían los nuevos órganos responsables de los ficheros y tratamientos asociados a esa función. Sin embargo, el Ministerio, órgano responsable hasta su traspaso, que había regulado la creación de un único fichero marco para todos los colegios en los que tenía competencia *(Gestión de centro docente),* en la Orden Ministerial de 1 de agosto de 2002, ha publicado la supresión de este fichero para crear un fichero por cada centro o colegio del territorio de Ceuta y Melilla, que mantienen la dependencia del Ministerio.

Por lo tanto, el resto de Comunidades Autónomas deberán proceder a publicar las correspondientes disposiciones reguladoras de creación de estos ficheros. En este sentido, el cambio de titularidad se ha visto reflejado en el año 2002 con la notificación realizada por la autoridad de control de la Comunidad de Madrid con base en las Ordenes 5181/2001, de 14 de noviembre (BOCM nº 281, de 26-11-2001) y 2545/2002, de 5 de junio (BOCM nº 148, de 24-6-2002) de la Consejería de Educación, que además, de establecer los ficheros de

cada órgano responsable ha supuesto que se produzca un incremento importante en el número de inscripciones por el hecho de haber optado por la publicación de tres ficheros marco por cada uno de los centros docentes no universitarios de su ámbito territorial, como ya se exponía anteriormente.

Si se mantuviera el criterio de la Comunidad de Madrid y de las Ciudades Autónomas de Ceuta y Melilla para el resto de Comunidades, se produciría un aumento considerable en el número de ficheros que constarían inscritos en el RGPD.

4.6. Transformación en la naturaleza jurídica del responsable

El cambio de la naturaleza jurídica de un Entre Institucional de la Administración Pública en una entidad de naturaleza jurídico-privada, implica una modificación registral en los correspondientes ficheros de datos personales.

En este caso, además del cambio de denominación del responsable, que es necesario a los efectos de dar publicidad del catálogo de ficheros existentes para facilitar el ejercicio de los derechos reconocidos por la LOPD al ciudadano, también se produce un cambio de titularidad, de ficheros de titularidad pública que pasan a depender de una entidad privada y por tanto, deben estar inscritos bajo esta titularidad. En este sentido, algunos principios de protección de datos son diferentes dependiendo de la titularidad del responsable del fichero. Además, los Capítulos Primero o Segundo del Título IV de la LOPD, establecen diferentes disposiciones sectoriales para los ficheros de titularidad pública y privada, respectivamente.

Si bien las nuevas inscripciones de titularidad privada no plantean mayores problemas que los propios de la cumplimentación de los modelos de notificación. Sin embargo, sí se plantea respecto de la supresión de la inscripción de los ficheros de titularidad pública, de conformidad con el art. 20 de la LOPD.

En este sentido, el art. 20 de la LOPD establece que la supresión de los ficheros de las Administraciones Públicas sólo puede hacerse mediante una disposición general publicada en el diario o boletín oficial correspondiente. No obstante, cuando un órgano ha perdido su dependencia orgánica y/o funcional de la Administración Pública tutelante y se convierte en una entidad privada, pierde su potestad reglamentaria, por lo que no tiene capacidad para publicar la disposición de supresión de los ficheros.

Es entonces necesario acudir a las normas que establecen el cambio de titularidad, en las que se refleja la conversión del organismo y se establece el mecanismo para proceder al traspaso de los bienes y servicios del mismo. Entendiendo que los ficheros de datos de

carácter personal forman parte de los bienes de la entidad y por lo tanto, al quedar suprimido el organismo público, se puede interpretar que la misma norma que suprime el organismo sería la norma que habilita la supresión de los ficheros para cumplir con la previsión del ya citado art. 20.

Por esta razón, no es posible aplicar a estas situaciones el procedimiento de modificación de las inscripciones, dado que al existir un cambio de titularidad, es necesario proceder a una nueva inscripción de los ficheros de titularidad privada y a la supresión simultánea de las inscripciones de los ficheros de titularidad pública.

Durante este año se ha producido esta situación con las inscripciones del organismo autónomo Correos y Telégrafos, que se ha transformado en la Entidad Pública Empresarial Correos y Telégrafos, S.A.

4.7. Procedimiento de inscripción de ficheros de titularidad pública

La inscripción de ficheros en el RGPD se regula por los siguientes preceptos legales:

- La creación, modificación o supresión de ficheros de titularidad pública sólo puede hacerse mediante una disposición general publicada en el boletín o diario oficial correspondiente (art. 20.1 LOPD)

- Las disposiciones de creación o de modificación deberán indicar a tenor del art. 20.2 LOPD, lo siguiente:

  a) La finalidad del fichero y los usos previstos para el mismo.
  b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
  c) El procedimiento de recogida de los datos de carácter personal.
  d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
  e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
  f) Los órganos de las Administraciones responsables del fichero.
  g) Los servicios o unidades ante los que se pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

- Las disposiciones de supresión de los ficheros establecerán el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción (art. 20.3 LOPD).

- Serán objeto de inscripción en el Registro General de Protección de Datos los ficheros de que sean titulares las Administraciones Públicas (art. 39.2.a) LOPD).

- Son objeto de inscripción en el RGPD los ficheros que contengan datos personales y de los que sean titulares:

  a) La Administración General del Estado.
  b) Las entidades y organismos de la Seguridad Social.
  c) Los organismos autónomos del Estado, cualquiera que sea su clasificación.
  d) Las sociedades estatales y entes del sector público.
  e) Las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes.
  f) Las entidades que integran la Administración Local y los entes y organismos dependientes de la misma.
  g) Cualesquiera otras personas jurídico-públicas, físicas o jurídicas.

- Todo fichero de titularidad pública debe ser notificado a la Agencia por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el modelo normalizado elaborado por la Agencia, acompañado de una copia de la disposición de creación del fichero (art. 5 del Real Decreto 1332/1994).

- Los ficheros de titularidad pública serán inscritos de oficio por la Agencia de Protección de Datos, una vez haya recibido la copia de la disposición de creación del fichero (art. 7.1 Real Decreto 1332/1994).

- En los asientos de inscripción de los ficheros de titularidad pública figurará, en todo caso, la información contenida en la disposición general de creación o modificación del fichero, de conformidad con lo previsto en el art. 20 de la LOPD (art. 24.2 del Real Decreto 428/1993).

- En los ficheros de titularidad pública, la inscripción contendrá las indicaciones previstas en el artículo 20.2 de la LOPD, con la especificación de la disposición general de creación y del diario oficial de su publicación (art. 7.3 Real Decreto 1332/1994).

- El Director de la Agencia puede resolver sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos (art. 12.2 del Real Decreto 428/1993).

- El art. 44.3.a) determina que 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 BOE o diario oficial correspondiente, constituye una infracción grave.

Los órganos responsables de ficheros de titularidad pública, con carácter general, mantienen un comportamiento muy parecido, independientemente de su pertenencia a una u otra Administración Pública. En un primer momento, cumplen con la obligación formal de notificar la creación de los ficheros que se encuentran en su ámbito de responsabilidad, previa la publicación de la disposición general de creación, según lo establecido en el art. 20 de la LOPD y en el art. 5 del Real Decreto 1332/1994. Sin embargo, con posterioridad no notifican al Registro las modificaciones que se puedan producir posteriormente en estos ficheros.

La falta de cumplimiento de todos los trámites previstos en la Ley y sus reglamentos da lugar a que la inscripción no se actualice y el Registro pierda su exactitud, en detrimento del derecho fundamental del ciudadano en relación con la protección de sus datos personales.

Como ya citábamos anteriormente, cuando se publican las disposiciones y no se notifican a la Agencia de Protección de Datos, se produce una inconsistencia y desactualización en la información inscrita. En 2002, la Administración General del Estado ha publicado las disposiciones de carácter general que se relacionan en el apartado correspondiente de esta Memoria. Sin embargo, al cierre del ejercicio, únicamente se han notificado en su totalidad los ficheros correspondientes a la Dirección General de la Policía.

En otros casos, sí se notifican las modificaciones pero, sin embargo, se detectan irregularidades en la declaración que dificultan la actualización del Registro. Principalmente se refieren a la falta de adecuación de la disposición general a los requisitos previstos en el art. 20 de la LOPD, y que la información consignada en la notificación no se corresponde con lo publicado en la disposición, y al amparo legal para la realización de comunicaciones de datos a terceros.

Por otra parte, dado que la disposición debe contener todos los apartados señalados en el art. 20.2 de la LODP, cabe señalar que su aprobación ha introducido una modificación en el contenido de la regulación normativa con respecto a lo previsto en la LORTAD, ya que debe indicarse el nivel básico, medio o alto que deben cumplir las medidas de seguridad aplicables al fichero, y, en su caso, los destinatarios de las transferencias internacionales de datos.

A continuación se relacionan los problemas más frecuentes que se han detectado en la tramitación de la disposición de creación, modificación o supresión de un fichero de titularidad pública y que no se detectan hasta el momento de notificar los ficheros al RGPD.

- La norma habilitante no tiene la consideración de disposición de carácter general exigida por la Ley.

- El contenido no se ajusta a las previsiones del art. 20.2 de la LOPD, al no publicar el nivel de medidas de seguridad.

Cuando se presenta alguna de estas situaciones, que se producen con relativa frecuencia, no se puede proceder a la inscripción de oficio del fichero, por lo que es necesario requerir al órgano responsable e informarle de los aspectos a subsanar. Esto supone, normalmente, un retraso importante, toda vez que implica la corrección de la disposición y su nueva publicación.

Además acontece que normalmente no se ha previsto, en el momento que se inicia el desarrollo tecnológico del proyecto, la necesidad de una habilitación legal para tratar los datos personales, lo que da lugar a que se puedan estar tratando datos personales sin haber cumplido con lo señalado en el art. 20.1 en la primera etapa de implantación del proyecto.

El cambio de la organización de los órganos responsables de ficheros produce dificultades para la correcta identificación de los titulares de los mismos. Esto conlleva el cambio de denominación del responsable de los ficheros asociados a cada centro directivo afectado por la reestructuración. Es criterio a la APD que la propia norma que establece la nueva estructura debe tener la consideración de disposición general, en relación con el apartado f) del art. 20.2 que establece que *«Las disposiciones de creación o de modificación de ficheros deberán indicar los órganos de las Administraciones responsables del fichero».*

Por lo tanto, únicamente sería necesario notificar los nuevos datos de identificación del responsable y, en su caso, del servicio o unidad ante el que ejercitar los derechos reconocidos por la LOPD, todo ello en cumplimiento del art. 5 del Real Decreto 1332/1994.

En la práctica, esta situación no se comunica en la mayoría de los casos, por lo que de nuevo se ve menoscabada la función del Registro de facilitar al ciudadano la dirección dónde ejercitar sus derechos. A estos efectos, la Agencia periódicamente recuerda a los responsables la situación de la inscripción de sus ficheros y solicita que se actualice la misma.

Vista la problemática existente con la aplicación de la LOPD en lo relativo a la inscripción de ficheros, y con la práctica de los años de funcionamiento de la APD, se plantean algunas propuestas que podrían dotar de mayor agilidad y fiabilidad al procedimiento de notificación.

En primer lugar, toda vez que la tramitación de una disposición general que habilite la creación de ficheros de titularidad pública es excesivamente compleja, sería conveniente que las normas legales que desarrollan el funcionamiento de determinados órganos de la Admi-

nistración, que necesitan tratar datos personales para alcanzar sus objetivos, incluyeran las previsiones establecidas en el art. 20 de la LOPD.

En este sentido, existen importantes ficheros a los que les es de aplicación una legislación específica, este es el caso del Padrón Municipal de Habitantes, Registros de Población, Registros administrativos, que podrían estar amparados por las propias normas de desarrollo, de esta manera complementarían las previsiones exigidas en el art. 20 de la LOPD.

En segundo lugar, hasta el momento, para poder cumplir con esta previsión es necesario que cada responsable haya procedido a la publicación individual de la disposición general de creación del fichero. Al estar definidos en las normas de desarrollo los diferentes aspectos que regulan el funcionamiento de estos órganos sería más sencillo incluir las distintas previsiones del artículo 20 y tan sólo quedaría el trámite de proceder a su notificación para su inscripción.

4.8. Disposiciones de carácter general de creación, modificación y supresión de ficheros de las Administraciones Públicas

Durante 2002 en el ámbito de la Administración General del Estado han sido publicadas las disposiciones generales de creación, modificación o supresión de ficheros que se indican a continuación:

- Ministerio de Justicia:
  - Orden de 23 de enero de 2002, por la que se da publicidad a la Instrucción nº 6/2001, de la Fiscalía General del Estado, sobre creación de ficheros automatizados de datos personales gestionados por el Ministerio Fiscal (BOE nº 34, 8-2-2002).

- Ministerio de Hacienda:
  - Orden de 16 de octubre de 2002, por la que se modifica la Orden de 21 de diciembre de 1999 que aprueba la relación de ficheros automatizados de datos de carácter personal de la Agencia Estatal de Administración Tributaria (BOE nº 256, 25-10-2002).
  - Orden de 7 de junio de 2002, por la que se regulan los ficheros automatizados de datos de carácter personal existentes en el Ministerio de Hacienda y en determinados Organismos Públicos adscritos al mismo (BOE nº 153, 27-6-2002).

- Ministerio del Interior:
  - Corrección de errores a la Orden de 20 de junio de 2002, por la que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal, adecuándolos a las previsiones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y demás normativa sobre la materia (BOE nº 184, 2-8-2002).

— Orden de 20 de junio de 2002, por la que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal, adecuándolos a las previsiones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y demás normativa sobre la materia (BOE nº 165, 11-7-2002).
— Orden de 11 de junio de 2002, por la que se regula el fichero automatizado (CAPGC) para la elección de miembros del Consejo Asesor de Personal del Cuerpo de la Guardia Civil (BOE nº 152, 26-6-2002).
— Orden de 7 de febrero de 2002, de modificación del anexo de la Orden de 5 de febrero de 2001, por la cual se crean en la Delegación del Gobierno, para el Plan Nacional sobre Drogas, diversos ficheros automatizados de datos de carácter personal (BOE nº 63, 14-3-2002).

- Ministerio de Fomento:
  — Orden de 20 de mayo de 2002, por la que se actualiza la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento (BOE nº 135, 6-6-2002).

- Ministerio de Educación, Cultura y Deporte:
  — Orden de 1 de agosto de 2002, por la que se regulan los ficheros automatizados con datos de carácter personal del Ministerio de Educación, Cultura y Deporte y sus organismos autónomos (BOE nº 193, 13-8-2002).

- Ministerio de Trabajo y Asuntos Sociales:
  — Resolución de 23 de julio de 2002, del Instituto Nacional de Seguridad e Higiene en el Trabajo, por la que se regulan los ficheros automatizados de datos de carácter personal de este Instituto Nacional (BOE nº 211, 3-9-2002).
  — Orden de 4 de marzo de 2002, 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 70, 22-3-2002).

- Ministerio de la Presidencia:
  — Corrección de errores de la 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 47, 23-2-2002).

- Ministerio de Sanidad y Consumo:
  — Orden de 23 de mayo de 2002, por la que se suprime el fichero automatizado de datos de carácter personal, «DIRCA» gestionado por el Ministerio de Sanidad y Consumo (BOE nº 132, 3-6-2002).

— Orden de 26 de febrero de 2002, por la que se amplía la de 21 de julio de 1994, que regula los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo (BOE nº 65, 16-3-2002).

- Ministerio de Economía:
  — Orden de 10 de enero de 2002, por la que se regulan los ficheros automatizados de datos de carácter personal de la organización central y de determinados organismos públicos adscritos al Ministerio de Economía (BOE nº 26, 30-1-2002).

- Ministerio de Ciencia y Tecnología:
  — Orden de 28 de noviembre de 2002, por la que se regulan los ficheros de datos de carácter personal del Departamento y de los organismos públicos de investigación dependientes del mismo (BOE nº 298, 13-12-2002).
  — Orden de 16 de julio de 2002, por la que se regulan los ficheros de datos de carácter personal de la Oficina Española de Patentes y Marcas (BOE nº 184, 2-8-2002).

- Consejo de Seguridad Nuclear:
  — Resolución de 30 de octubre de 2002, del Consejo de Seguridad Nuclear, por la que se regulan nuevos ficheros de tratamiento automatizado de datos de carácter personal existentes en el organismo: Destinatarios de publicaciones, visitantes y datos médicos (BOE nº 310, 27-12-2002).

- Banco de España:
  — Circular de 25 de enero de 2002, por la que se modifica la Circular de 22 de julio de 1994, sobre ficheros con datos de carácter personal gestionados por el Banco de España (BOE nº 34, 8-2-2002).

Por otra parte, también se recogen las disposiciones publicadas en los diarios o boletines de las diferentes Comunidades Autónomas que han sido remitidas a la APD:

- Comunidad Autónoma de Andalucía:
  — Orden de 9 de abril de 2002, de la Consejería de Agricultura y Pesca (BOJA nº 50, 30-4-2002).
  — Orden de 9 de abril de 2002, de la Consejería de Empleo y Desarrollo Tecnológico (BOJA nº 3, 8-1-2002).
  — Orden de 19 de marzo de 2002, de la Consejería de Empleo y Desarrollo Tecnológico (BOJA nº 46, 20-4-2002).
  — Orden de 24 de septiembre de 2002, de la Consejería de Justicia y Administración Pública (BOJA nº 124, 24-10-2002).
  — Orden de 30 de julio de 2002, de la Consejería de Obras Públicas y Transportes (BOJA nº 95, 13-8-2002).

– Orden de 28 de diciembre de 2001, de la Consejería de Salud (BOJA nº 12, 29-1-2002).
– Orden de 13 de mayo de 2002, de la Consejería de Salud (BOJA nº 68, de 11-6-2002).

- Comunidad Autónoma de Cantabria:
  – Orden de 13 de mayo de 2002, la Consejería de Presidencia (BOCA nº 93, de 16-5-2002).

- Comunidad Autónoma de Castilla-La Mancha:
  – Orden de 20 de julio de 2001, de la Consejería de Agricultura y Medio Ambiente (DOCM nº 34, de 8-2-2002).
  – Orden de 29 de Mayo de 2001, de la Consejería de Educación y Cultura (DOCM nº 67, de 8-6-2002).

- Comunidad Autónoma de Castilla y León:
  – Orden de 7 de agosto de 2002, de la Consejería de Educación y Cultura (BOCL nº 167, de 29-8-2002).

- Comunidad Autónoma de Cataluña:
  – Disposición de 29 de julio de 2002, del Departamento de Sanidad y Seguridad Social (DOGC nº 3695, de 2-8-2002).

- Comunidad Autónoma de Galicia:
  – Orden de 27 de febrero de 2003, de la Consejería de Asuntos Sociales, Empleo y Relaciones Laborales (DOGA nº 50, de 12-3-3003).
  – Resolución de 25 de febrero de 2002, de la Consejería de Economía y Hacienda (DOGA nº 44, de 1-3-2002).
  – Orden de 1 de febrero de 2002, de la Consejería de Industria y Comercio (DOGA nº 31, de 12-2-2002).
  – Orden de 6 de noviembre de 2002, de la Consejería de Sanidad (DOGA nº 231, de 29-11-2002).
  – Orden de 25 de enero de 2002, de la Consejería de Sanidad (DOGA nº 38, de 21-2-2002).

- Comunidad de Madrid:
  – Orden 10 de 29 de julio de 2002, de la Consejería de Economía e Innovación Tecnológica (BOCM nº 100, de 29-4-2002).
  – Orden 6119 de 13 de diciembre de 2001 de la Consejería de Educación (BOCM nº 9, de 11-1-2002).
  – Orden 2545 de 5 de junio de 2002, de la Consejería de Educación (BOCM nº 148, de 24-6-2002).

— Orden 3956 de 21 de agosto de 2002, de la Consejería de Educación (BOCM nº 210, de 4-9-2002).
— Orden 6118 de 13 de diciembre de 2001 de la Consejería de Educación (BOCM nº 9, de 11-1-2002).
— Orden de 27 de febrero de 2002, de la Consejería de Hacienda (BOCM nº 60, de 12-3-2002).
— Orden de 15 de octubre de 2002, de la Consejería de Justicia y Administraciones Públicas (BOCM nº 250, de 21-10-2002).
— Orden 755 de 2 de julio de 2002, de la Consejería de las Artes (BOCM nº 164, de 12-7-2002).
— Orden 1010 de 9 de septiembre de 2002, de la Consejería de las Artes (BOCM nº 222, de 18-9-2002).
— Orden 223 de 20 de marzo de 2002, de la Consejería de las Artes (BOCM nº 78, de 3-4-2002).
— Orden 985 de 7 de mayo de 2002, de la Consejería de Medio Ambiente (BOCM nº 116, de 17-5-2002).
— Orden 4678 de 27 de diciembre de 2001 de la Consejería de Medio Ambiente (BOCM nº 13, de 16-1-2002).
— Orden 148 de 31 de enero de 2002, de la Consejería de Medio Ambiente (BOCM nº 32, de 7-2-2002).
— Orden 198 de 8 de febrero de 2002, de la Consejería de Medio Ambiente (BOCM nº 45, de 22-2-2002).
— Orden de 31 de enero de 2002, de la Consejería de Obras Públicas, Urbanismo y Transportes (BOCM nº 41, de 18-2-2002).
— Orden de 6 de febrero de 2002, de la Consejería de Obras Públicas, Urbanismo y Transportes (BOCM nº 41, de 18-2-2002).
— Decreto 99 de 13 de junio de 2002, de la Consejería de la Presidencia (BOCM nº 145, de 20-6-2002).
— Orden 394 de 5 de junio de 2002, de la Consejería de Sanidad (BOCM nº 143, de 18-6-2002).

- Comunidad Foral de Navarra:
  — Orden foral 122 de 25 de abril de 2002, de la Consejería de Educación y Cultura (BON nº 70, de 10-6-2002).
  — Decreto foral 152 de 22 de julio de 2002 del Departamento de Agricultura, Ganadería y Alimentación (BON nº 110, de 11-9-2002).
  — Orden foral 40 de 8 de febrero de 2002 del Departamento de Economía y Hacienda (BON nº 157, de 30-12-2002).
  — Decreto foral 152 de 22 de julio de 2002 del Departamento de Educación y Cultura (BON nº 110, de 11-9-2002).
  — Orden foral 384 de 19 de julio de 2002 del Departamento de Educación y Cultura (BON nº 113, de 18-9-2002).

– Orden foral 30 de 8 de febrero de 2002 del Departamento de Educación y Cultura (BON nº 39, de 29-3-2002).
– Decreto foral 152 de 22 de julio de 2002 del Departamento de Presidencia (BON nº 110, de 11-9-2002).
– Orden foral 364 de 29 de octubre de 2001 del Departamento de Presidencia, Justicia e Interior (BON nº 16, de 6-2-2002).
– Orden foral 406 de 26 de diciembre del Departamento de Presidencia, Justicia e Interior (BON nº 15, de 4-2-2002).
– Orden foral 67 de 21 de junio de 2002 del Departamento de Presidencia, Justicia e Interior (BON nº 79, de 1-7-2002).
– Decreto foral 152 de 22 de julio de 2002 del Departamento de Salud (BON nº 110, de 11-9-2002).
– Resolución de 24 de junio de 2002, de la Consejería de Administraciones Públicas y Asuntos Europeos (BON nº 165, de 17-7-2002).

- Comunidad Autónoma de la Rioja:
  – Orden 6 de 2 de abril de 2002, de la Consejería de Salud y Servicios Sociales (BOLR nº 45, de 13-4-2002).
  – Orden 10 de 29 de julio de 2002, de la Consejería de Salud y Servicios Sociales (BOLR nº 97, de 10-8-2002).

- Comunidad Valenciana:
  – Orden de 10 de julio de 2002, de la Consejería de Bienestar Social (DOGV nº 4303, de 30-7-2002).
  – Orden de 11 de febrero de 2002, de la Consejería de Economía, Hacienda y Empleo (DOGV nº 4193, de 19-2-2002).
  – Orden de la Consejería de Innovación y Competitividad (DOGV nº 4192, de 18-2-2002).
  – Orden de 21 de diciembre de 2001 de la Consejería de Justicia y Administraciones Públicas (DOGV nº 4182, de 4-2-2002).
  – Orden de 15 de enero de 2002, de la Consejería de Medio Ambiente (DOGV nº 4234, de 23-4-2002).
  – Orden de 8 de mayo de 2002, de la Consejería de Obras Públicas, Urbanismo y Transportes (DOGV nº 4262, de 3-6-2002).
  – Orden de 16 de septiembre de 2002, de la Consejería de Portavoz del Gobierno (DOGV nº 4343, de 30-9-2002).
  – Orden de 10 de junio de 2002, de la Consejería de Sanidad (DOGV nº 4285, de 4-7-2002).
  – Orden de 26 de marzo de 2002, de la Consejería de Economía, Hacienda y Empleo (DOGV nº 4234, de 23-4-2002).
  – Orden de 21 de junio de 2002, de la Consejería de Economía, Hacienda y Empleo (DOGV nº 4284, de 3-7-2002).

— Orden de 8 de marzo de 2002, de la Consejería de Innovación y Competitividad (DOGV nº 4221, de 4-4-2002).
— Resolución de 24 de abril de 2002, de la Presidencia de la Generalitat Valenciana (DOGV nº 4245, de 9-5-2002).
— Corrección de errores de la Resolución de 24 de abril de 2002, de la Presidencia de la Generalitat Valenciana (DOGV nº 4268 de 11-6-2002).
— Resolución de 7 de Junio de 2002, de la Presidencia de la Generalitat Valenciana (DOGV nº 4272, de 17-6-2002).
— Resolución de 5 de agosto de 2002, de la Presidencia de la Generalitat Valenciana (DOGV nº 4315, de 16-8-2002).

5. Transferencias Internacionales de Datos

5.1. Notificación del apartado de Transferencias Internacionales

Los artículos 33 y 34 de la LOPD, establecen el régimen al que habrán de someterse los movimientos internacionales de datos.

El artículo 33 prohíbe las transferencias de datos con destino a países que no proporcionan un nivel de protección equiparable al que presta nuestra Ley, y lo hace en términos muy parecidos a los previstos en el artículo 25 de la Directiva 95/46/CE.

No obstante, el segundo inciso del apartado 1 del artículo 33, permite que se pueda obtener una autorización del Director de la APD, que sólo podrá otorgarse si se obtienen garantías adecuadas.

El carácter equiparable del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia; en particular, se tendrá en consideración la naturaleza de los datos, la finalidad, la duración del tratamiento, el país de origen y el país de destino final, las normas de Derecho vigentes en el país tercero, así como las normas profesionales y las medidas de seguridad vigentes en dichos países.

La APD considera que se aportan garantías suficientes cuando las mismas se deriven, en particular, de cláusulas contractuales apropiadas. En este sentido, se consideran cláusulas contractuales apropiadas las publicadas en las Decisiones de la Comisión Europea: 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la trans-

misión de datos a terceros países y 2002/16/CE, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos a los encargados de tratamiento establecidos en terceros países.

Cuando se pretenda realizar una transferencia internacional a países con protección no adecuada amparándose en las garantías estipuladas en las Decisiones citadas, será necesario que se solicite una autorización de transferencia internacional y se presente copia del contrato que estipule las garantías para poder dar trámite a la solicitud de autorización. En el siguiente apartado se expone un resumen de las autorizaciones de transferencia internacional que se han tramitado durante el año 2002.

Por lo tanto, con carácter general habrá de estarse a lo dispuesto en el artículo 33 de la LOPD. No obstante, el artículo 34, establece las excepciones a la norma general. Estas excepciones están reflejadas en los diferentes supuestos que aparecen preimpresos en el apartado 12 de *transferencias internacionales* del modelo de notificación de inscripción de ficheros.

Los supuestos previstos en el artículo 34 para poder realizar transferencias, a países considerados como no adecuados, sin necesidad de solicitar una autorización, son los siguientes:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos 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.

Hay que hacer una mención singular al apartado k) de este artículo, que garantiza que no será necesario realizar ningún trámite de autorización cuando la transferencia tenga como destinatario un Estado miembro de la Unión Europea o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado.

Los responsables de ficheros y tratamientos que realicen transferencias amparándose en alguno de los supuestos citados anteriormente, no necesitarán solicitar autorización, y únicamente deberán cumplir con la previsión de notificar el apartado de transferencia internacional, a los efectos de su inscripción, según dispone el artículo 26 de la LOPD, como uno más de los extremos exigidos en la notificación de ficheros.

Con mayor razón, no necesitarán ningún trámite de autorización, las transferencias a países de la Comunidad Económica Europea, y a países que se consideren con un nivel de protección adecuado, aunque sí será necesario que se comuniquen a los efectos de la notificación de los ficheros.

En este sentido y hasta la fecha, garantizan un nivel de protección equivalente, los estados miembros de la Comunidad Económica Europea o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, estando incluidos, entre estos últimos, Suiza, Hungría, las entidades estadounidenses adheridas a los «principios de Puerto Seguro» y Canadá respecto de las entidades canadienses de ámbito federal.[4]

Es necesario hacer una mención especial a Argentina, próximo país que la Comisión declarará de nivel adecuado y que al cierre de esta memoria, aún no se ha publicado la adecuación de la protección proporcionada a dicho país.

En la tabla siguiente figura un resumen de los ficheros inscritos en el RGPD durante 2002, que han declarado transferencias internacionales de datos, exceptuadas a tenor del artículo 34 de la LOPD:

---

[4] Ver apartado de esta Memoria Aspectos Internacionales de la Protección de Datos. Análisis de las Tendencias Legislativas, Jurisprudenciales y Doctrinales, en relación con la Orden de 2 de febrero de 1995 por la que se aprobó la relación de países con protección adecuada que puede entenderse derogada por ser contraria a la LOPD.

SUPUESTOS LEGALES (un mismo fichero puede estar amparado en varios supuestos)	TITULARIDAD PÚBLICA	TITULARIDAD PRIVADA
Se ampara en tratado o convenio del que España forma parte	30	268
Se realiza a efectos de prestar auxilio judicial internacional	27	11
Es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios	3	24
Se refiere a transferencias dinerarias, conforme a su legislación específica	2	25
El afectado ha dado su consentimiento inequívoco	7	519
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	314
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	3	269
Es necesaria o legalmente exigida para la salvaguarda de un interés público	3	8
Es precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial	5	30
Se efectúa, a petición de persona con interés legítimo, desde un registro público y es acorde con la finalidad del mismo	4	17
Se efectúa con destino a algún país que proporciona un nivel de protección equiparable	33	724

El total de ficheros inscritos con transferencias 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.

A continuación, por su interés, se van a resaltar una serie de casos en los que las transferencias quedan amparadas por alguno de los supuestos del artículo 34, y por lo tanto, se han inscrito en el RGPD sin necesidad de autorización.

5.2. Casos singulares excepcionados de autorización

Candidatos participantes en procesos de selección

El responsable es una entidad que se dedica a la selección de personal para grupos multinacionales.

La transferencia se notifica consignando el supuesto del artículo 34.e) de la LOPD, de consentimiento inequívoco a la transferencia y la necesidad de la transferencia para la adopción de medidas precontractuales adoptadas a petición del afectado.

El consentimiento se recaba a través de una cláusula incluida en la primera comunicación que el departamento de selección de la entidad le envía al candidato, y por la cual se acusa recibo de la recepción del *«curriculum vitae»* y se le informa de que se va a iniciar el proceso de selección.

El motivo por el que justifica la necesidad de la transferencia es la iniciación de los trámites de selección, que pueden resultar en la contratación del candidato como empleado, teniendo en cuenta que la entidad es una firma internacional que puede desarrollar su actividad en el área de su influencia constituida por países de protección no adecuada.

Asimismo, se considera que cuando el candidato pase a ser empleado deberá participar en proyectos que se desarrollen en estos países, en colaboración con las sociedades establecidas en aquellos territorios. Por lo tanto, a la hora de evaluar candidatos y de determinar la adecuación del candidato a los perfiles específicos que se requieren en cada momento, es necesario tener en cuenta los datos de los mismos para que pueda evaluarse la adecuación del candidato al perfil del puesto.

Así mismo, se considera que el afectado al enviar un *«curriculum»,* está interesado en entrar a formar parte de una organización multinacional y entiende que sus datos necesariamente van a tener que ser transferidos, para poder comprobar la adecuación de su perfil profesional a las necesidades de la empresa.

Prestación de servicios de Hosting

El responsable es una entidad española que se dedica a prestar servicio de correo electrónico y que ha contratado a una entidad establecida en un tercer país la prestación de servicios de *hosting* de correo web para sus propios usuarios (clientes).

La transferencia se notifica amparada en la «Existencia del consentimiento inequívoco a la transferencia».

Este consentimiento se recaba a través de la web. Antes de efectuar de manera automatizada el alta de usuario en el servidor del tercer país, de forma clara y antes del botón de «Enviar», se informa al usuario que debe estar conforme, entre otras, con la política de privacidad y las condiciones de uso.

Existe un epígrafe donde se dice *«El servicio de correo está gestionado por una tercera empresa..., al darse de alta en el servicio de correo web... el usuario es consciente que una copia de sus datos (cuenta creada, nombre o alias, contraseña) será almacenada en los servidores de la tercera empresa que está ubicada..., país que no tiene nivel de protección de*

datos equiparable al de España. Esta transferencia se realiza única y exclusivamente por razones técnicas al ser imprescindible para la prestación del servicio, cuyo hosting se realiza en esos servidores».

Esta situación es muy común, con los proveedores meramente técnicos, en aquellos tratamientos que se realizan en Internet. Normalmente los servidores donde se aloja la información suelen ser de terceros.

En estos casos, además de notificar la transferencia que se produce para que se realice un tratamiento por cuenta de terceros, la misma deberá estar regulada en un contrato en los términos del artículo 12 de la LOPD.

Prestación de asistencia sanitaria, repatriaciones y traslados de restos mortales

El responsable es una entidad española de seguros y reaseguros que para dar dicho servicio, utiliza una red de hospitales, médicos, servicios de ambulancias, urgencias, funerarias, compañías de aviación y compañías de asistencia. En cada caso, a cada proveedor se le comunica la información necesaria para que puedan dar la asistencia necesaria a las personas.

La transferencia se notifica amparada en los supuestos de que es necesaria para la prevención o para el diagnóstico médicos, el consentimiento inequívoco a la transferencia y que es necesaria para la celebración de un contrato en interés del afectado.

Gestión de transferencias dinerarias con el exterior

El responsable es un establecimiento de cambio de moneda inscrito en el registro del Banco de España.

La transferencia se ampara en el supuesto d) del artículo 34 cuando se refiera a transferencias dinerarias conforme a la legislación específica.

La legislación específica que regula la actividad de la entidad se encuentra recogida en el Real Decreto 2660/1998 de 14 de diciembre sobre el cambio de moneda extranjera en establecimientos abiertos al público distintos de las Entidades de Crédito, y en las Órdenes de 16 de noviembre de 2000 de regulación de determinados aspectos del régimen jurídico de los establecimientos de cambio de moneda y sus agentes, y de desarrollo de la Ley 9/1999 de 12 de abril, por la que se regula el régimen jurídico de las transferencias entre Estados miembros de la Unión Europea.

Estudios de investigación (ensayos clínicos multicéntricos internacionales)

El responsable del fichero es un laboratorio farmacéutico. Los ensayos clínicos se llevan a cabo de conformidad con lo dispuesto en la normativa nacional y las directrices internacionales. Según esta normativa los ensayos clínicos deben contar con las oportunas autorizaciones de las autoridades sanitarias, en España y Estados Unidos, para lo que es preciso aportar y cumplimentar una serie de documentos que contienen datos personales de los investigadores.

La cesión de estos datos a Estados Unidos, se ampara en el supuesto del consentimiento inequívoco a la transferencia.

El investigador, al firmar el protocolo (donde consta que el ensayo es de ámbito internacional) está dando su consentimiento inequívoco a la transferencia prevista.

Autorización de comercialización de un medicamento

El responsable del fichero es un laboratorio farmacéutico.

Los datos de los expertos se recaban con el fin de dar cumplimiento a la obligación de acompañar a la solicitud de autorización de comercialización de un medicamento, el informe de experto.

En el caso de que un laboratorio pretenda registrar una especialidad farmacéutica en otro país, deberá acompañar entre otra documentación, el informe de experto que en su día hubiese realizado respecto al medicamento en cuestión.

El laboratorio informa al experto, en el momento de contratar sus servicios, en qué países va a solicitar posteriormente la autorización de la especialidad farmacéutica, obteniendo su consentimiento expreso e inequívoco para poder ceder sus datos a las autoridades sanitarias de los países en cuestión.

Candidatos demandantes de empleo que se dan de alta en el servicio de bolsa de empleo de una institución pública o privada a través de un Portal de empleo

El responsable es una entidad que se dedica a la selección de personal.

La transferencia se notifica consignando el supuesto de consentimiento inequívoco a la transferencia de datos.

La entidad es la persona jurídica que recaba los datos, los almacena en sus servidores, los trata en una base de datos y realiza el seguimiento de los mismos, para prestar su servicio a los usuarios que buscan empleo en la web de una institución, realizando dicha actividad dentro del marco de un acuerdo de colaboración celebrado con la institución.

La finalidad es el cruce entre curriculums de demandantes de empleo y las ofertas de empleo que las empresas y particulares asociados a la institución publican en su página web.

Los candidatos demandantes de empleo que se den de alta en el servicio de bolsa de empleo prestan el consentimiento a los términos de uso y el compromiso de privacidad, con carácter previo a la introducción de sus datos de carácter personal en la web.

Para la recepción del mencionado consentimiento del candidato a los términos de uso y al compromiso de privacidad, y por ende a las transferencias internacionales de sus datos de carácter personal han creado un sistema de cifrado, que controla el acceso del usuario al formulario de entrada de datos de carácter personal, y que impide automáticamente aquellos accesos en los que el usuario no presta su consentimiento o presta un consentimiento defectuoso.

5.3. Autorizaciones de Transferencias Internacionales

Como se ha dicho anteriormente, el artículo 33 de la LOPD establece que para realizar transferencias internacionales de datos a países con nivel de protección no adecuado, será necesario solicitar una autorización del Director de la APD. Esta autorización solo podrá ser otorgada si, además de cumplir con lo dispuesto en la LOPD, se obtienen las garantías adecuadas.

Dicha autorización será otorgada en caso de que el responsable del fichero aporte un contrato celebrado o a celebrar entre el transmitente y el destinatario, en el que consten las garantías necesarias, en los términos previstos en las Decisiones de la Comisión de la Unión Europea, citadas anteriormente, relativas a las cláusulas contractuales tipo para la transferencia internacional de datos personales a un tercer país y a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.

Durante el año 2002 se han tramitado cuatro expedientes de autorización de transferencia internacional procediéndose, al amparo del artículo 33 de la Ley, a autorizar todas las solicitadas.

En todas las autorizaciones de transferencias resueltas, los destinatarios realizan una prestación de servicio al responsable del tratamiento. La realización de tratamiento por parte de estos encargados de tratamiento está regulada en los contratos aportados que vinculan al encargado con el responsable del tratamiento, que además de en los términos que se exigen en el artículo 12 de la Ley, completan estos contratos con todas las cláusulas exigidas por la Comisión.

Las autorizaciones han sido otorgadas toda vez que los responsables de los ficheros han aportado un contrato entre el transmitente y el destinatario, en el que constan las garantías necesarias.

En este sentido, cabe reseñar las siguientes cláusulas:

1. La finalidad de la transferencia es la prestación de servicios, en los términos previstos en el artículo 12 de la LOPD.

2. El exportador de los datos, como responsable de los ficheros, asume plenamente las garantías de cumplimiento de todas las obligaciones y derechos dispuestos en la Ley, respetando íntegramente las normas contenidas en la LOPD.

3. El importador se compromete a que los datos de carácter personal que se van a transferir, no van a ser utilizados más que para la finalidad que motiva las transferencias y en ningún caso se comunicarán o cederán total o parcialmente a terceros, sin el consentimiento de los afectados.

4. En cuanto a las medidas de seguridad, tanto el exportador como el importador de los datos cumplirán estrictamente las obligaciones que se establecen en el artículo 9 de la LOPD, habiendo implementado las oportunas medidas de índole técnica y organizativa para evitar su alteración, pérdida y tratamiento o acceso no autorizado, garantizando asimismo la seguridad de los datos. Asimismo se garantiza que se cumple lo estipulado 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 de datos de carácter personal.

5. Tanto el exportador como el importador de los datos responderán solidariamente frente a los particulares, a la APD y a los Órganos Jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudieran incurrir los receptores, cuando los mismos sean constitutivos de infracción de lo dispuesto en la LOPD o produzcan un perjuicio a los afectados.

6. Se indemnizará al afectado que resulte perjudicado como consecuencia del tratamiento efectuado por el importador de los datos.

7. El exportador de los datos garantiza que los afectados podrán ejercitar los derechos de oposición, acceso, rectificación y cancelación desde España y ante el responsable del fichero. Asimismo, el interesado podrá recabar la tutela de la Agencia de Protección de Datos en los supuestos previstos en la LOPD, en caso de que sus derechos no sean atendidos.

8. El importador de los datos garantiza el compromiso de cooperar con la autoridad de control competente en el curso de todas sus consultas y acatar sus consejos. Por lo tanto, cooperará con la APD en todas las funciones que ésta desarrolle, incluyendo la inspección y el reconocimiento de las resoluciones que dicte.

9. El exportador de los datos, como responsable del fichero, mantiene el poder de decisión sobre el tratamiento de los datos y el importador de los datos únicamente actuará siguiendo las instrucciones del importador. Ambas partes asumen lo dispuesto en el artículo 43 de la LOPD, quedando sujetas, como responsable de los ficheros la primera y como encargado del tratamiento la segunda, al régimen sancionador establecido en la LOPD.

Dos de las autorizaciones resueltas durante el año 2002 han sido obtenidas por empresas pertenecientes al mismo grupo empresarial y tienen como país de destino, los Estados Unidos de América.

La finalidad de estas dos transferencias autorizadas fue la prestación de servicios de tratamiento automatizado para la realización de contratos nuevos, mantenimiento de la cartera de contratos y clientes, gestiones de impagos, gestión de cobros, gestión de personal y gestión de pagos a proveedores, por parte de una entidad del mismo grupo empresarial, ubicada en Estados Unidos.

Los datos objeto de la transferencia son de carácter identificativo del cliente, proveedor o empleado y financieros del cliente, necesarios para la consecución de las actividades objeto de la finalidad de la transferencia.

En las otras dos transferencias autorizadas coincide el país de destino, Argentina, y la entidad encargada del tratamiento en dicho país. Las entidades españolas se dedican, entre otras actividades, a la de venta a distancia a través de los distintos canales establecidos al efecto y la entidad argentina está especializada en la prestación de servicios de emisión y recepción de llamadas, servicios denominados genéricamente de *«Call Center».*

La finalidad de la transferencia es la prestación de servicios consistentes en la emisión de llamadas a los clientes, para ofrecerles los productos y servicios que comercializan las entidades españolas. Los datos objeto de la transferencia son de carácter identificativo del cliente.

En estos casos, las bases de datos siguen estando ubicadas en territorio español y únicamente el encargado de tratamiento en Argentina tiene acceso *«on-line»* a las mismas.

En estas transferencias, debe tenerse en consideración que la República Argentina, con la aprobación de la Ley de Habeas Data y el Decreto, de 3 de diciembre de 2001, que además de desarrollar otros aspectos de la Ley, regula la creación de la autoridad de control argen-

tina, Dirección Nacional de Protección de Datos, garantiza el cumplimiento de la protección de datos de carácter personal con una legislación muy similar a la española. Asimismo, en la actualidad se está tramitando por la Comisión de las Comunidades Europeas, la adecuación de la protección proporcionada en Argentina a fin de satisfacer los requisitos del artículo 25 de la Directiva 95/46/CE.

Todas las autorizaciones de transferencia internacional de datos de carácter personal han sido notificadas a la Comisión y a los demás Estados miembros en cumplimiento del artículo 26. 3 de la Directiva 95/46/CE.

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 a 31 de diciembre de 2002. 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.

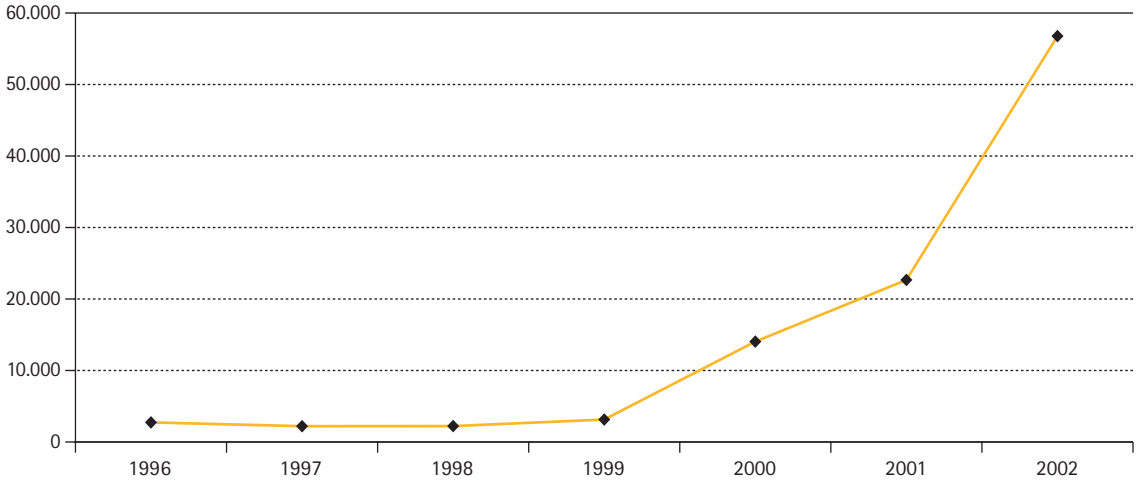
A fecha 31 de diciembre de 2002, el número de ficheros inscritos en el RGPD era de 328.649, de los cuales 35.894 correspondían a inscripciones de titularidad pública y 292.755 a inscripciones de titularidad privada.

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

Se recoge en la siguiente tabla la evolución del número de ficheros inscritos en el Registro General de Protección de Datos que constaban a 31 de diciembre de cada año, de acuerdo con los datos que aparecen en las diferentes Memorias Anuales de la Agencia desde 1994, según la titularidad de los mismos.

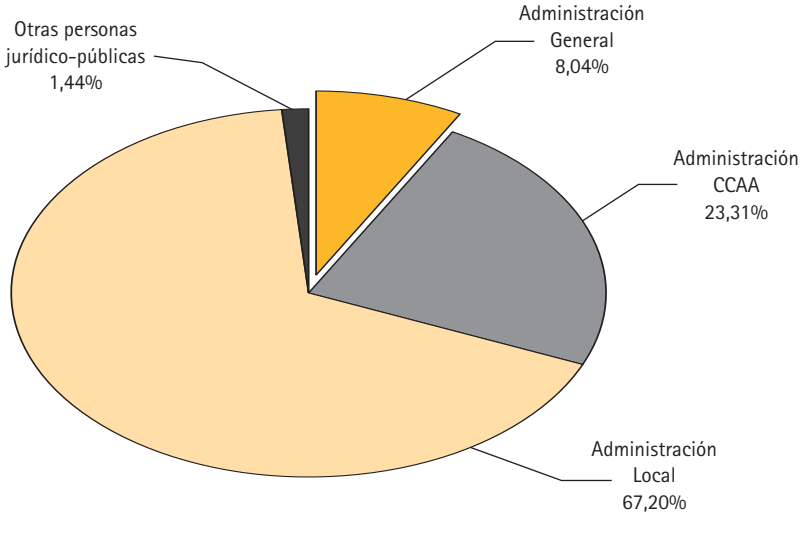
	A 31/12/94	A 31/12/95	A 31/12/96	A 31/12/97	A 31/12/98	A 31/12/99	A 31/12/00	A 31/12/01	A 31/12/02
Titularidad pública	20.198	24.923	26.541	27.969	28.890	30.431	31.155	31.805	35.894
Titularidad privada	192.097	199.933	201.054	201.835	203.138	204.737	218.054	240.070	292.755
TOTAL	**212.295**	**224.856**	**227.595**	**229.804**	**232.028**	**235.168**	**249.209**	**271.875**	**328.649**

INCREMENTO ANUAL INSCRIPCIÓN



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

	TOTAL
Administración General	2.887
Administración CC.AA.	8.368
Administración Local	24.121
Otras personas jurídico-públicas	518
TOTAL	**35.894**



DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA DE LA ADMINISTRACIÓN GENERAL INSCRITOS EN EL RGPD

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

	TOTAL
Presidencia del Gobierno	7
Ministerio de Asuntos Exteriores	522
Ministerio de Justicia	22
Ministerio de Defensa	39
Ministerio de Hacienda	170
Ministerio del Interior	189
Ministerio de Fomento	222
Ministerio de Educación, Cultura y Deporte	135
Ministerio de Trabajo y Asuntos Sociales	308
Ministerio Portavoz del Gobierno	3
Ministerio de Agricultura, Pesca y Alimentación	38
Ministerio de la Presidencia	42
Ministerio de Administraciones Públicas	215
Ministerio de Sanidad y Consumo	652
Ministerio de Medio Ambiente	164
Ministerio de Economía	102
Ministerio de Ciencia y Tecnología	57
TOTAL	**2.887**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA DE LA ADMINISTRACIÓN DE LAS COMUNIDADES AUTÓNOMAS 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 AUTÓNOMA	TOTAL
Comunidad Autónoma de Andalucía	572
Comunidad Autónoma de Aragón	178
Comunidad Autónoma de Canarias	255
Comunidad Autónoma de Cantabria	27
Comunidad Autónoma de Castilla-La Mancha	116
Comunidad Autónoma de Castilla y León	228
Comunidad Autónoma de Cataluña	522
Ciudad Autónoma de Ceuta	23
Comunidad Valenciana	391
Comunidad Autónoma de Extremadura	64
Comunidad Autónoma de Galicia	557
Comunidad Autónoma de las Illes Balears	31
Comunidad Autónoma de La Rioja	208
Comunidad de Madrid[5]	4.395
Ciudad Autónoma de Melilla	62
Comunidad Foral de Navarra	105
Comunidad Autónoma del País Vasco	335
Comunidad Autónoma del Principado de Asturias	144
Comunidad Autónoma de la Región de Murcia	155
TOTAL	**8.368**

[5] El número de inscripciones, en la Comunidad de Madrid, se ha debido a la realización de notificaciones por cada uno de los centros docentes de su ámbito territorial.

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA DE LA ADMINISTRACIÓN 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	FICHEROS
Comunidad Autónoma de Andalucía	**707**	**5.574**
Almería	104	951
Cádiz	49	335
Córdoba	63	283
Granada	169	1.184
Huelva	85	1.150
Jaén	84	487
Málaga	54	418
Sevilla	99	766
Comunidad Autónoma de Aragón	**434**	**1.969**
Huesca	156	536
Teruel	45	154
Zaragoza	233	1.279
Comunidad Autónoma de Canarias	**89**	**521**
Las Palmas	46	254
Santa Cruz de Tenerife	43	247
Comunidad Autónoma de Cantabria	**44**	**197**
Comunidad Autónoma de Castilla-La Mancha	**349**	**1.880**
Albacete	74	356
Ciudad Real	108	558
Cuenca	82	556
Guadalajara	11	58
Toledo	74	352
Comunidad Autónoma de Castilla y León	**505**	**2.241**
Ávila	8	28
Burgos	93	326
León	165	810
Palencia	18	77
Salamanca	80	339
Segovia	14	104
Soria	9	31
Valladolid	83	369
Zamora	35	157

	ENTIDADES	FICHEROS
Comunidad Autónoma de Cataluña	**588**	**2.775**
Barcelona	334	1.533
Girona	59	400
Lleida	109	407
Tarragona	86	435
Comunidad Valenciana	**323**	**2.054**
Alicante	139	1.015
Castellón de la Plana	35	226
Valencia	149	813
Comunidad Autónoma de Extremadura	**193**	**1.578**
Badajoz	157	1.397
Cáceres	36	181
Comunidad Autónoma de Galicia	**233**	**959**
A Coruña	88	443
Lugo	45	175
Ourense	38	147
Pontevedra	62	194
Comunidad Autónoma de las Illes Balears	**67**	**649**
Comunidad Autónoma de La Rioja	**29**	**157**
Comunidad de Madrid	**60**	**741**
Comunidad Foral de Navarra	**84**	**408**
Comunidad Autónoma del País Vasco	**198**	**1.673**
Álava	55	253
Guipúzcoa	69	759
Vizcaya	74	661
Comunidad Autónoma del Principado de Asturias	**52**	**314**
Comunidad Autónoma de la Region de Murcia	**39**	**431**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD

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

	RESPONSABLES	FICHEROS INSCRITOS
Comunidad Autónoma de Andalucía	**13.779**	**27.095**
Almería	655	1.351
Cádiz	2.061	3.732
Córdoba	1.532	3.450
Granada	1.104	2.203
Huelva	756	1.282
Jaén	1.007	2.241
Málaga	4.242	7.158
Sevilla	2.442	5.678
Comunidad Autónoma de Aragón	**8.801**	**15.310**
Huesca	2.002	2.979
Teruel	613	1.040
Zaragoza	6.192	11.291
Comunidad Autónoma de Canarias	**2.497**	**6.677**
Las Palmas	1.433	3.855
Santa Cruz de Tenerife	1.070	2.822
Comunidad Autónoma de Cantabria	**771**	**2.029**
Comunidad Autónoma de Castilla-La Mancha	**3.438**	**7.089**
Albacete	1.031	1.778
Ciudad Real	737	1.677
Cuenca	554	976
Guadalajara	261	613
Toledo	856	2.045
Comunidad Autónoma de Castilla y León	**5.354**	**11.105**
Ávila	251	484
Burgos	1.409	2.642
León	759	1.636
Palencia	294	661
Salamanca	624	1.403
Segovia	323	574
Soria	266	418
Valladolid	1.149	2.509
Zamora	286	778

	RESPONSABLES	FICHEROS INSCRITOS
Comunidad Autónoma de Cataluña	**39.570**	**80.225**
Barcelona	29.879	61.964
Girona	3.468	6.466
Lleida	3.638	6.743
Tarragona	2.634	5.052
Ciudad Autónoma de Ceuta	**71**	**148**
Comunidad Valenciana	**16.829**	**30.677**
Alicante	6.349	10.791
Castellón de la Plana	2.653	5.114
Valencia	7.840	14.772
Comunidad Autónoma de Extremadura	**2.681**	**4.792**
Badajoz	2.094	3.571
Cáceres	589	1.221
Comunidad Autónoma de Galicia	**7.285**	**14.697**
A Coruña	3.867	8.102
Lugo	920	1.523
Ourense	620	1.242
Pontevedra	1.884	3.830
Comunidad Autónoma de las Illes Balears	**1.628**	**4.325**
Comunidad Autónoma de La Rioja	**1.807**	**3.616**
Comunidad de Madrid	**22.034**	**57.815**
Ciudad Autónoma de Melilla	**40**	**64**
Comunidad Foral de Navarra	**1.885**	**3.924**
Comunidad Autónoma del País Vasco	**4.893**	**11.258**
Álava	769	1.832
Guipúzcoa	2.185	4.762
Vizcaya	1.948	4.664
Comunidad Autónoma del Principado de Asturias	**2.367**	**5.302**
Comunidad Autónoma de la Región de Murcia	**3.658**	**6.584**

FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD DE RESPONSABLES ESTABLECIDOS FUERA DEL TERRITORIO ESPAÑOL

	EMPRESAS	FICHEROS
Responsables en la Unión Europea	**15**	**20**
Francia	5	10
Italia	1	1
Reino Unido	8	8
Suecia	1	1
Responsables en terceros países	**3**	**3**
Estados Unidos	2	2
Suiza	1	1

DISTRIBUCIÓN DE FICHEROS SEGÚN LA TIPOLOGÍA DE DATOS QUE CONTIENEN

	TITULARIDAD PÚBLICA	TITULARIDAD PRIVADA
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	247	3.115
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	2.376	32.054
Datos relativos a infracciones	1.392	(*)
Datos de carácter identificativo	35.894	292.755
Datos de características personales	19.646	120.459
Datos de circunstancias sociales	9.485	34.126
Datos académicos y profesionales	13.029	43.506
Detalles de empleo y carrera administrativa	9.200	94.820
Datos de información comercial	7.110	49.729
Datos económico-financieros	15.454	140.955
Datos de transacciones	5.938	78.256

(*) No aplicable a esta titularidad.

DISTRIBUCIÓN DE FICHEROS INSCRITOS CON DATOS SENSIBLES

	TITULARIDAD PÚBLICA	TITULARIDAD PRIVADA
Datos especialmente protegidos	**247**	**3.115**
Ideología	38	218
Creencias	25	135
Religión	138	815
Afiliación Sindical	67	2.310
Otros datos especialmente protegidos	**2.376**	**32.054**
Origen Racial	113	258
Salud	2.353	32.012
Vida Sexual	505	501
Datos relativos a infracciones	**1.392**	(*)
Infracciones Penales	787	(*)
Infracciones Administrativas	1.068	(*)

(*) No aplicable a esta titularidad.

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

	TOTAL
Recursos humanos	
Gestión de personal	5.984
Gestión de nómina (*)	163
Formación de personal	1.489
Acción social a favor del personal de las Admones. Públicas	863
Promoción y selección de personal, oposiciones y concursos (*)	70
Prevención de riesgos laborales (*)	41
Control horario	68
Control de incompatibilidades	676
Control de patrimonio de altos cargos públicos	227
Hacienda y gestión económico-financiera	
Gestión tributaria y de recaudación	6.901
Gestión económica y contable	7.001
Gestión de facturación (*)	1.135
Gestión fiscal (*)	152
Gestión deuda pública y tesorería	2.520
Gestión de catastros inmobiliarios rústicos y urbanos	1.892
Relaciones comerciales con el exterior	847
Regulación de mercados financieros	33
Defensa de la competencia	27
Justicia	
Procedimientos judiciales	1.051
Registros vinculados con la fe pública (*)	46
Prestación social sustitutoria	849
Tramitación de indultos	264
Seguridad pública y defensa	
Protección civil	1.684
Seguridad vial	1.373
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	2.079
Actuaciones de fuerzas y cuerpos de seguridad con fines administrativos	1.872
Gestión y control de centros e instituciones penitenciarias	328
Tramitación servicio militar	2.132
Solicitudes de visado/residencia (*)	6
Trabajo y bienestar social	
Promoción y gestión de empleo	906
Relaciones laborales y condiciones de trabajo	1.407
Inspección y control de seguridad y protección social	707
Formación profesional ocupacional	1.119
Prestaciones a desempleados	1.007
Prestaciones de garantía salarial	307
Prestaciones de asistencia social	1.764

	TOTAL
Pensiones, subsidios y otras prestaciones económicas	2.021
Acción a favor de inmigrantes	442
Servicios sociales a minusválidos	834
Servicios sociales a la tercera edad	1.119
Promoción social a la mujer	662
Promoción social a la juventud	707
Protección del menor	806
Acción a favor de toxicómanos (*)	26
Ayudas acceso a vivienda	1.081
Otros servicios sociales	1.210
Sanidad	
Gestión y control sanitario	1.760
Historial clínico	908
Investigación epidemiológica y actividades análogas	1.215
Gestión de tarjeta sanitaria (*)	7
Educación y cultura	
Enseñanza infantil y primaria	1.383
Enseñanza secundaria	1.298
Enseñanza superior	473
Enseñanzas artísticas e idiomas	707
Educación especial	374
Becas y ayudas a estudiantes	2.092
Deportes	916
Fomento y apoyo a actividades artísticas y culturales	969
Protección del patrimonio histórico artístico	110
Estadística	
Función estadística pública	8.110
Padrón de habitantes	4.505
Encuestas sociológicas y de opinión	171
Finalidades varias	
Procedimientos administrativos	12.121
Registro de entrada y salida de documentos (*)	142
Otros registros administrativos (*)	151
Atención al ciudadano (*)	362
Concesión y gestión de permisos, licencias y autorizaciones	3.493
Seguridad y control de acceso a edificios	2.057
Publicaciones	674
Fines científicos, históricos o estadísticos (*)	83
Gestión sancionadora	2.388
Gestión de estadísticas internas	12.314
Prestación de servicios de certificación (*)	141
Otras finalidades	4.534

(*) Finalidades que se incluyeron en el 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

	TOTAL
Gestión contable, fiscal y administrativa	
Gestión económica y contable	163.263
Gestión fiscal	152.626
Gestión administrativa	170.445
Gestión de facturación (*)	26.300
Gestión de clientes	97.196
Gestión de proveedores (*)	17.358
Gestión de cobros y pagos	117.574
Administración de fincas (*)	736
Consultorías, auditorías, asesorías y servicios relacionados	17.150
Históricos de relaciones comerciales	42.582
Recursos humanos	
Gestión de personal	67.923
Gestión de nóminas	14.136
Formación de personal	6.010
Prestaciones sociales	18.484
Selección de personal	7.997
Gestión de trabajo temporal (*)	1.157
Promoción y gestión de empleo (*)	1.827
Prevención riesgos laborales (*)	3.425
Control horario (*)	3.067
Servicios económico-financieros y seguros	
Cuenta de crédito	4.787
Cuenta de depósito	2.729
Gestión de patrimonios	2.438
Gestión de fondos de pensiones y similares	2.525
Gestión de tarjetas de crédito y similares	1.715
Registro de acciones y obligaciones	2.361
Otros servicios financieros	4.322
Cumplimiento/incumplimiento de obligaciones dinerarias (*)	730
Prestación de servicios de solvencia patrimonial y crédito	3.308
Seguros de vida y salud	7.708
Otro tipo de seguros	7.297
Publicidad y prospección comercial	
Publicidad propia	26.170
Venta a distancia (*)	3.833
Encuestas de opinión	5.633
Análisis de perfiles (*)	1.497
Prospección comercial	10.812
Segmentación de mercados (*)	1.660

	TOTAL
Sistemas de ayuda a la toma de decisiones (*)	1.911
Recopilación de direcciones (*)	2.180
Servicio de telecomunicaciones	
Prestación de servicios de telecomunicaciones	1.911
Guías/repertorios de servicios de telecomunicaciones (*)	186
Comercio electrónico (*)	972
Prestación de servicios de certificación (*)	72
Actividades asociativas, culturales, recreativas, deportivas y sociales	
Gestión de actividades culturales (*)	526
Gestión de clubes o asociaciones deportivas, culturales, profesionales y similares	3.151
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro (*)	574
Actividades asociativas diversas (*)	550
Asistencia social (*)	329
Gestión de medios de comunicación social	687
Educación	
Enseñanza infantil primaria	1.644
Enseñanza secundaria	1.744
Enseñanza universitaria	967
Educación especial	497
Otras enseñanzas	2.924
Sanidad	
Gestión y control sanitario	21.736
Historial clínico	13.600
Investigación epidemiológica y actividades análogas	3.012
Seguridad	
Investigaciones privadas a personas	128
Seguridad y control acceso a edificios	753
Seguridad	1.589
Finalidades varias	
Fidelización de clientes	6.280
Reservas y emisión de billetes	686
Fines históricos, científicos o estadísticos	58.683
Otras finalidades	23.732

(*) Finalidades que se incluyeron en el 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 PÚBLICA	TITULARIDAD PRIVADA
Procedencia de los datos		
El propio interesado o su representante legal	33.881	269.821
Otras personas distintas al afectado o su representante	5.407	7.008
Fuentes accesibles al público (*)	3.276	12.097
Censo Promocional	–	–
Guías y Servicios de Telecomunicaciones	36	1.740
Listas de personas pertenecientes a grupos profesionales	437	2.217
Diarios y Boletines Oficiales	48	1.144
Medios de Comunicación	27	1.690
Registros públicos	6.940	5.683
Entidad privada	3.870	29.171
Administraciones públicas	14.363	6.048
Procedimiento de recogida		
Encuestas o entrevistas	7.175	91.758
Formularios o cupones	30.946	121.525
Transmisión electrónica de datos	6.637	15.160
Otros procedimientos de recogida	5.489	106.174
Soporte		
Soporte papel	34.130	234.060
Soporte informático/magnético	14.881	57.729
Vía telemática	5.188	15.911
Otros soportes	3.232	46.327

(*) 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

	TOTAL FICHEROS CON CESIONES
Titularidad pública	21.773
Titularidad privada	56.671
TOTAL	**78.444**

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

	TITULARIDAD PUBLICA	TITULARIDAD PRIVADA
Existe consentimiento de los afectados	10.374	31.498
Existe una relacion juridica cuyo desarrollo, control y cumplimiento implica necesariamente la conexion del fichero con ficheros de terceros	4.564	27.576
Existe una norma reguladora que las autoriza	13.953	31.598
Se trata de datos recogidos de fuentes accesibles al público	4.854	3.167
Corresponden a competencias identicas o que versan sobre las mismas materias, ejercidas por otras Administraciones Públicas	14.063	(*)
Son datos obtenidos o elaborados con destino a otra Administración Pública	9.557	(*)
La comunicación tiene por objeto el tratamiento posterior de los datos con fines historicos, estadísticos o científicos	750	(*)

(*) 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.

DISTRIBUCIÓN DE FICHEROS INSCRITOS EN EL RGPD QUE DECLARAN TRANSFERENCIAS INTERNACIONALES

	TOTAL FICHEROS CON TRANSFERENCIAS
Titularidad pública	79
Titularidad privada	2.535
TOTAL	**2.614**

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

ARTÍCULO 34	TITULARIDAD PÚBLICA	TITULARIDAD PRIVADA
a) Se ampara en tratado o convenio del que España forma parte	60	357
b) Se realiza a efectos de prestar auxilio judicial internacional	27	8
c) Es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios	10	63
d) Se refiere a transferencias dinerarias, conforme a su legislación específica	16	119
e) El afectado ha dado su consentimiento	9	999
f) 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	482
g) 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	3	410
h) Es necesaria o legalmente exigida para la salvaguarda de un interés público	4	11
i) Es precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial	5	28
j) Se efectúa a petición de persona con interés legítimo, desde un registro público y es acorde con la finalidad del mismo	2	30
k) Se efectúa con destino a algún país que proporciona un nivel de protección equiparable	69	2.197

Los datos reflejados en la tabla anterior no son sumables, ya que un mismo fichero inscrito puede estar amparado en más de un supuesto.

DISTRIBUCIÓN DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD DURANTE EL AÑO 2002

DOCUMENTOS DE ENTRADA	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Notificaciones inscripción	**1.534**	**1.673**	**1.544**	**1.649**	**1.918**	**2.635**	**6.476**	**3.290**	**2.635**	**3.005**	**3.193**	**3.373**	**32.925**
Soporte papel	251	346	407	439	538	816	2.235	854	666	862	649	578	8.641
Soporte magnético	202	123	157	288	357	544	745	464	312	582	380	523	4.677
Soporte internet	1.081	1.204	980	922	1.023	1.275	3.496	1.972	1.657	1.561	2.164	2.272	19.607
Otras solicitudes	**205**	**182**	**143**	**185**	**171**	**145**	**306**	**129**	**263**	**379**	**386**	**278**	**2.772**
TOTALES	**1.739**	**1.855**	**1.687**	**1.834**	**2.089**	**2.780**	**6.782**	**3.419**	**2.898**	**3.384**	**3.579**	**3.651**	**35.697**

REGISTROS DE SALIDA	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Resoluciones de inscripción	2.859	1.996	2.446	3.941	4.640	3.837	15.709	3.268	10.029	5.854	4.045	9.792	68.416
Requerimientos del RGPD	208	320	158	314	245	197	2.178	353	454	537	460	380	5.804
Salidas varias	87	87	96	94	87	145	253	64	175	329	167	231	1.815
TOTALES	**3.154**	**2.403**	**2.700**	**4.349**	**4.972**	**4.179**	**18.140**	**3.685**	**10.658**	**6.720**	**4.672**	**10.403**	**76.035**

El total de documentos de entrada correspondiente a notificaciones de inscripción no coincide con el total de operaciones de inscripción realizados en la base de datos, debido a que, una misma solicitud, puede contener varios movimientos de inscripción.

RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD DURANTE EL AÑO 2002

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Operaciones a instancia del interesado													
Altas	2.479	4.522	1.803	3.119	3.927	3.376	14.278	2.925	8.849	4.458	3.470	8.121	61.327
Modificaciones	470	271	470	1.299	438	320	806	260	683	935	370	890	7.212
Supresiones	172	228	246	426	325	178	680	96	526	577	270	818	4.542
TOTAL	**3.121**	**5.021**	**2.519**	**4.844**	**4.690**	**3.874**	**15.764**	**3.281**	**10.058**	**5.970**	**4.110**	**9.829**	**73.081**
Operaciones de subsanacion de oficio													
Modificaciones	68	82	216	353	193	345	480	315	769	524	277	315	3.937
Supresiones	0	0	1	1	0	0	2	0	1	6	0	0	11
TOTAL	**68**	**82**	**217**	**354**	**193**	**345**	**482**	**315**	**770**	**530**	**277**	**315**	**3.948**
TOTALES	**3.189**	**5.103**	**2.736**	**5.198**	**4.883**	**4.219**	**16.246**	**3.596**	**10.828**	**6.500**	**4.387**	**10.144**	**77.029**

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 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. Cumple así una función de gran importancia en orden a garantizar el respeto al derecho fundamental de protección de datos de carácter personal.

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 un 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.

Así mismo tramita los expedientes relativos a la aplicación del artículo 5.5 de la LOPD.

1.1. Expedientes relacionados con la función inspectora

En el ejercicio de la función inspectora realizada por la APD durante el año 2002 se iniciaron **723** 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 **723** actuaciones de inspección iniciadas durante 2002, **441** han finalizado en dicho ejercicio, estando el resto, **282**, pendientes de concluir. A las **441** actuaciones de inspección iniciadas y finalizadas en 2002 hay que añadir aquellas otras, en concreto **130**, que, iniciadas el año anterior, finalizaron en el presente año, lo que hace un total de **571** actuaciones de inspección terminadas en 2002.

Así mismo, y al margen de lo anterior, se han realizado durante el mismo año **67** 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 de la LOPD.

1.2. Expedientes relacionados con la función instructora

De las tres clases de procedimientos incoados en 2002 por los órganos instructores de la Inspección de Datos, **148** corresponden a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad privada; **13** a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública (procedimientos por infracciones de las Administraciones Públicas); y **447** se corresponden a los iniciados por procedimientos de tutela de derechos.

De los **148** procedimientos sancionadores iniciados durante el año 2002, han finalizado en dicho ejercicio **54**, estando el resto, **94,** pendientes de concluir. A los **54** procedimientos sancionadores iniciados y finalizados en el 2002 hay que añadir aquellos otros, en concreto **74**, que iniciados el año anterior finalizaron en el presente, lo que suma un total de **128** procedimientos sancionadores terminados en 2002.

De los **13** procedimientos por infracciones de las Administraciones Públicas iniciados en el 2002, **8** han finalizado en dicho año, estando los **5** restantes pendientes de conclusión. Así mismo, se han concluido durante el presente ejercicio **75** procedimientos de esta clase provenientes del año anterior, lo que supone la conclusión de **83** procedimientos por infracciones de las Administraciones Públicas en 2002.

A los anteriores procedimientos deben añadirse **240** 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 **3** 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 **447** procedimientos de tutela de derechos iniciados en 2002, **294** (3 de ellos fueron trasladados a la APD de la Comunidad de Madrid) han finalizado en el mismo ejercicio, quedando tan sólo **153** pendientes de concluir. A los **294** antes citados hay que añadir los procedimientos de esta clase iniciados el año anterior, en concreto **99**, y terminados en el presente, lo que hace un total de **393** procedimientos de tutela de derechos concluidos en el 2002.

A todos los procedimientos anteriores deben añadirse la resolución de **153** recursos de reposición, **2** recursos de alzada y **2** recursos extraordinarios de revisión, resueltos durante el mismo año 2002.

De los **153** recursos de esta clase presentados, **6** han sido estimados, **3** estimados parcialmente, **20** inadmitidos por extemporáneos o falta de legitimación y **124** desestimados por falta de fundamento de las pretensiones formuladas. No obstante, aún 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 2002 se han emitido un total de **1.005** resoluciones, que comprende la suma de los procedimientos sancionadores, resoluciones de archivo, actuaciones de colaboración con la CNIL, procedimientos de tutela de derechos, recursos de reposición, recursos de alzada, y recursos extraordinarios de revisión.

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 2002, 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

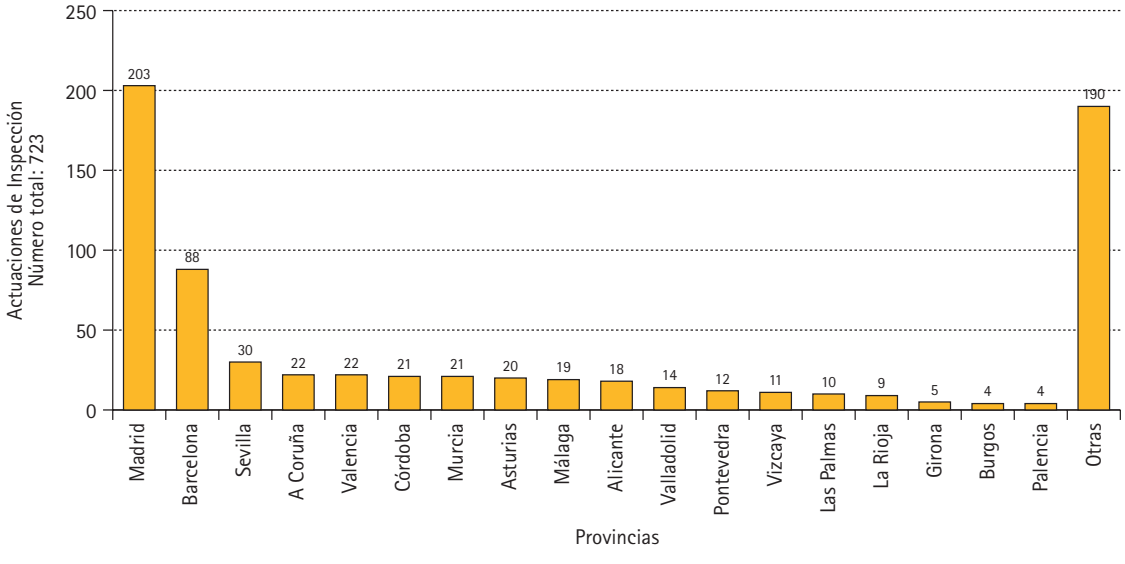


Gráfico II
ACTUACIONES DE INSPECCIÓN INICIADAS POR PROVINCIA DEL DENUNCIADO

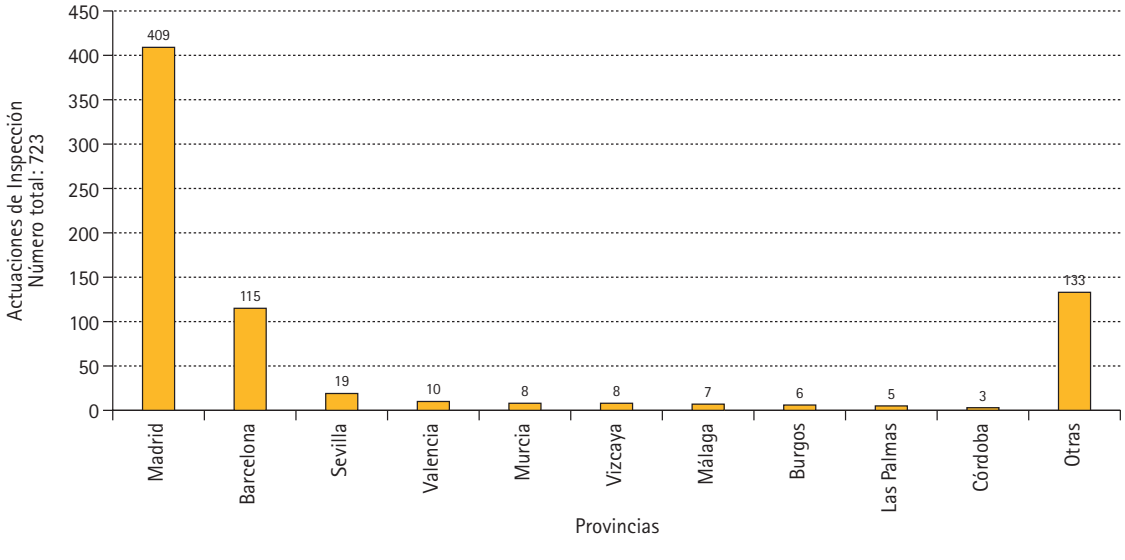
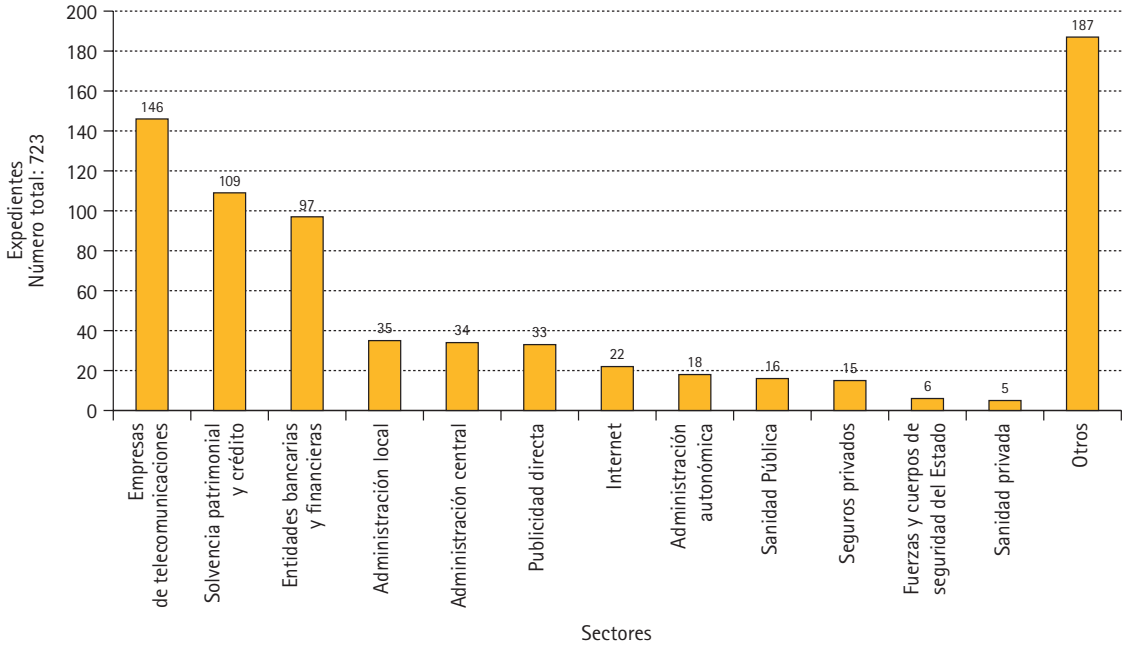
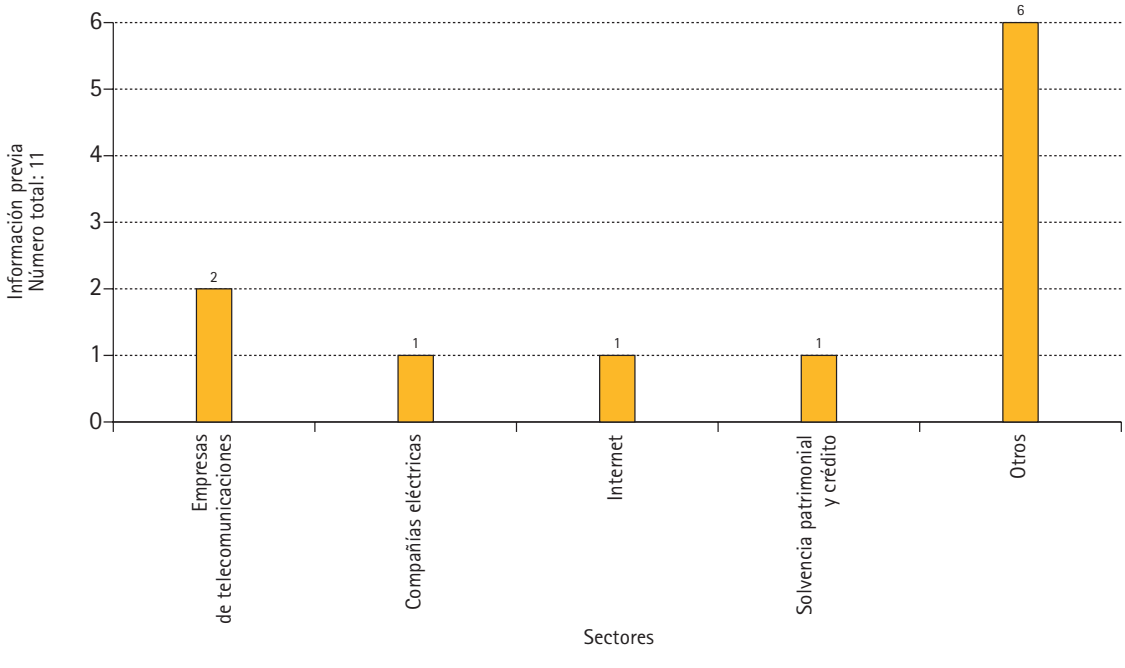


Gráfico III
ACTUACIONES DE INSPECCIÓN INICIADAS POR SECTORES DE ACTIVIDAD



A continuación, en el gráfico IV, se puede apreciar detalladamente la distribución por sectores de actividad de las actuaciones de información previa realizadas en 2002 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 2002 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

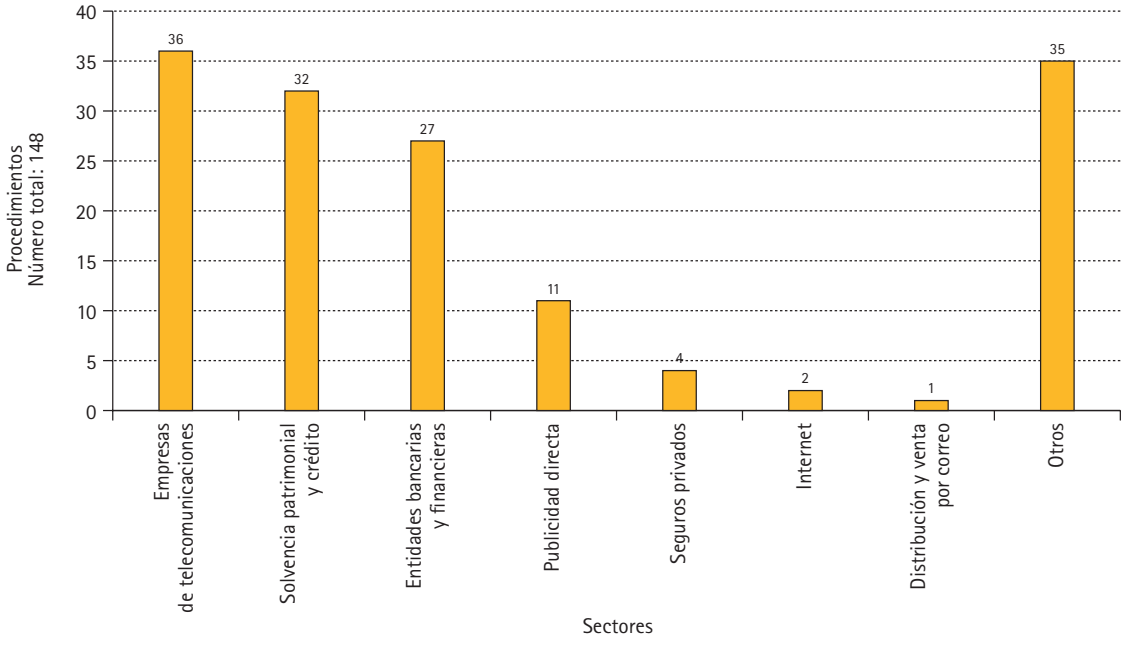


Gráfico V Bis
PROCEDIMIENTOS SANCIONADORES INICIADOS POR PROVINCIAS

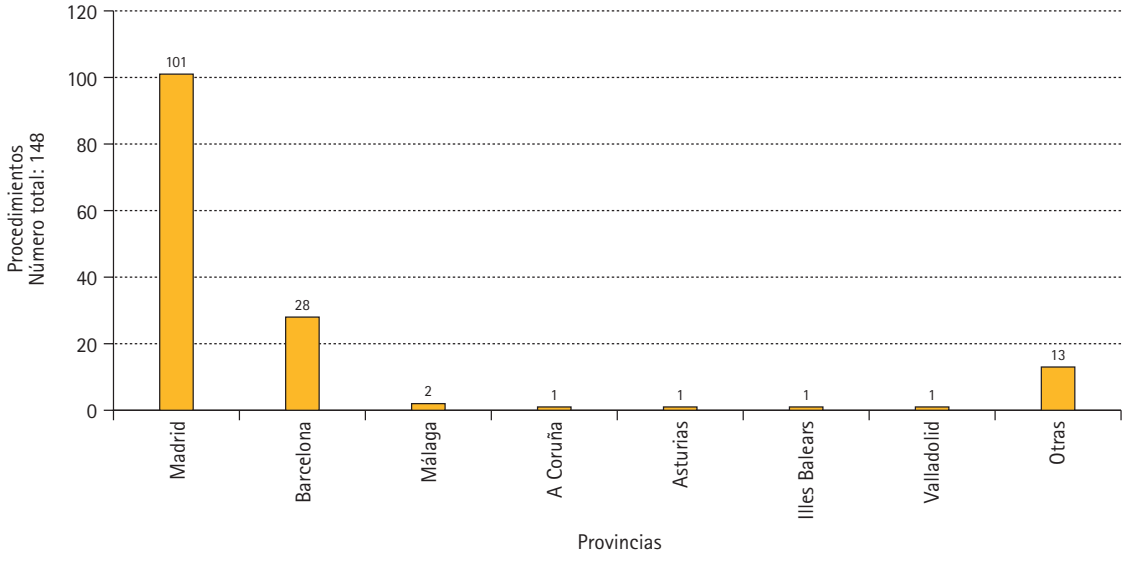


Gráfico VI
PROCEDIMIENTOS DE LAS AAPP INICIADOS POR SECTORES

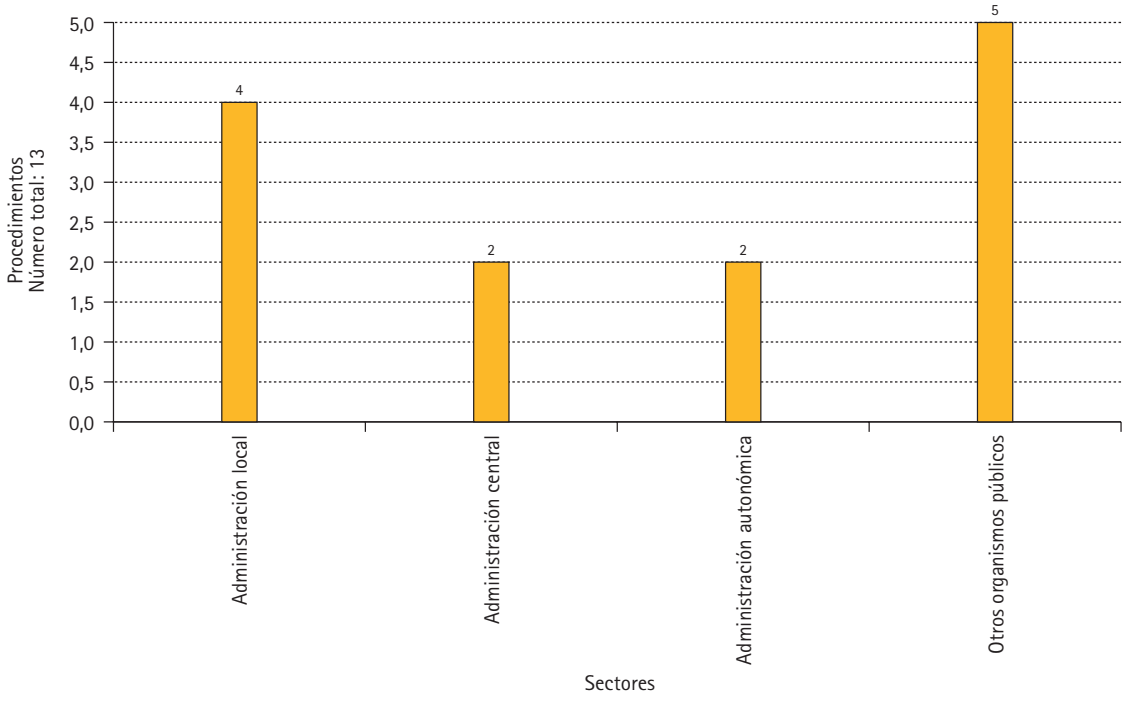


Gráfico VI Bis
PROCEDIMIENTOS DE LAS AAPP INICIADOS POR PROVINCIAS

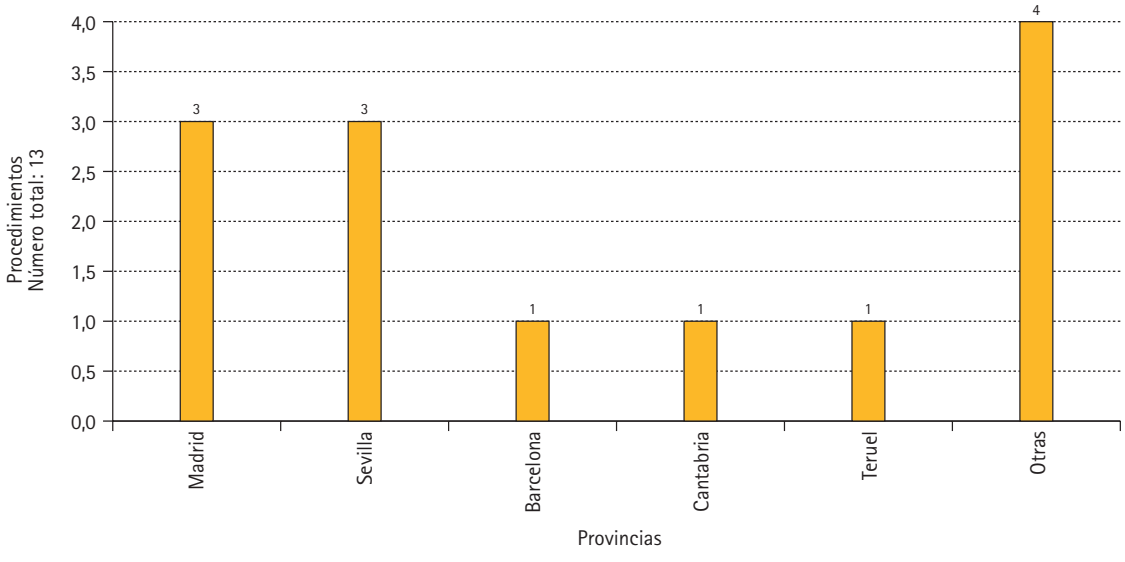


Gráfico VII
PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR SECTORES

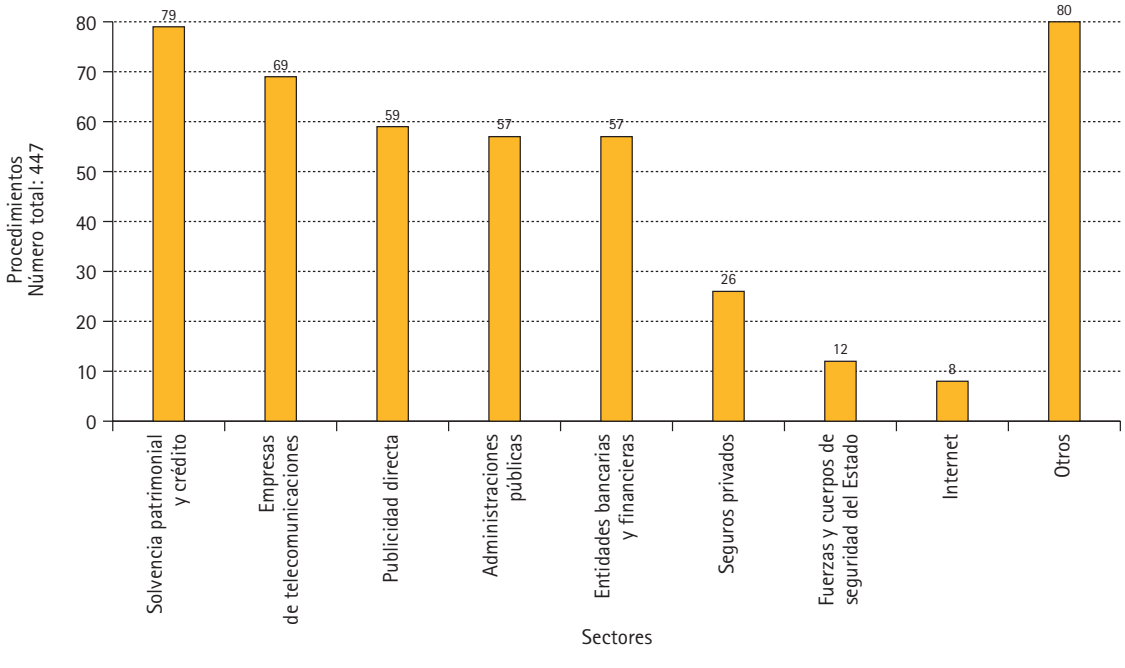
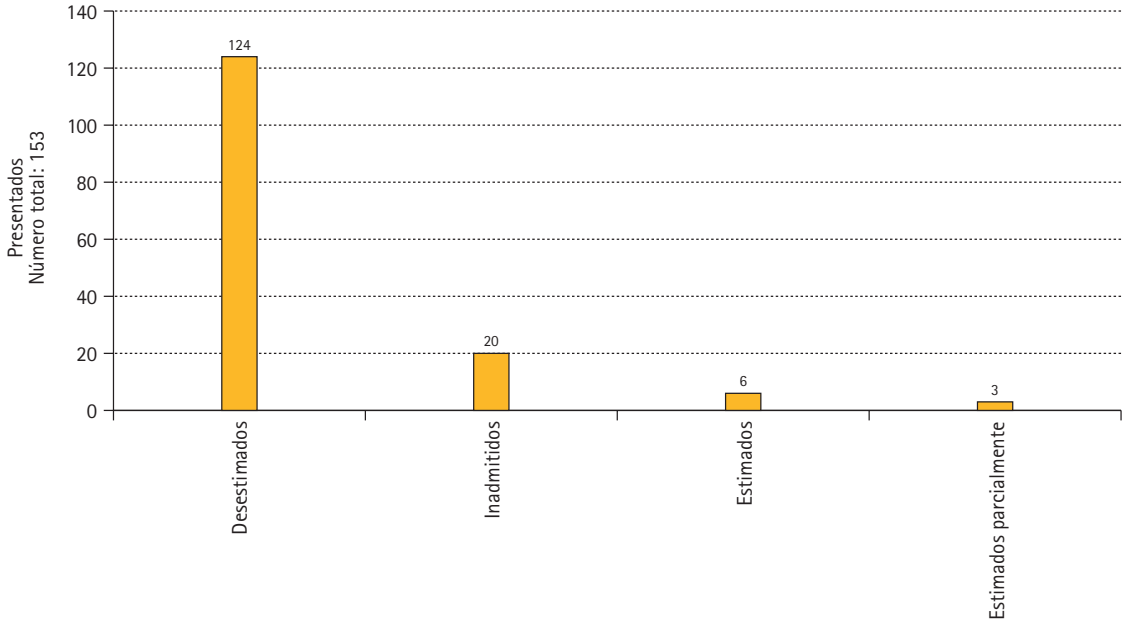
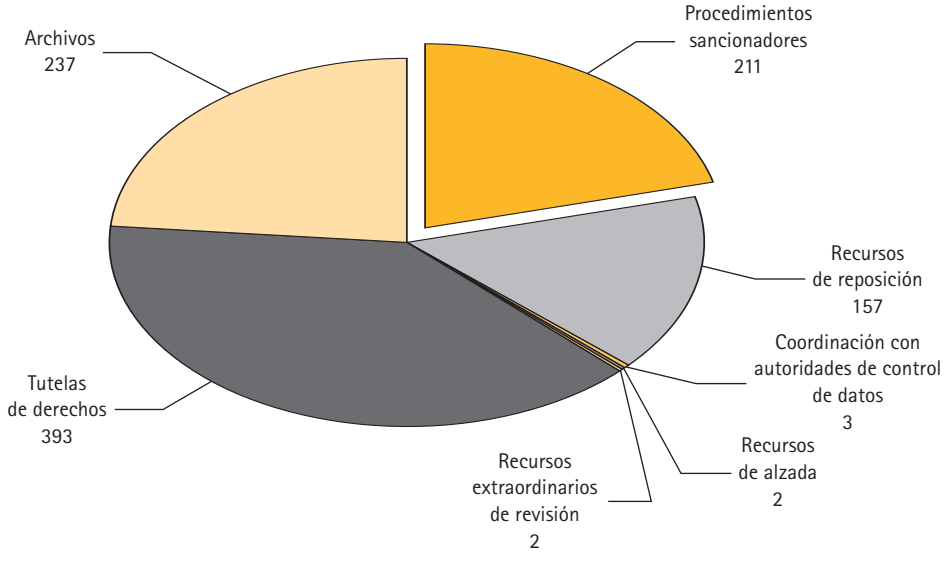


Gráfico VIII
RECURSO DE REPOSICIÓN



Por último, en el gráfico IX se presentan el total de resoluciones correspondientes a los procedimientos terminados durante el año 2002.



2. Planes Sectoriales de Oficio

Con objeto de facilitar el cumplimiento de la LOPD la Agencia continuó con el desarrollo de los llamados Planes Sectoriales de Oficio, que tienen como finalidad verificar la situación real de cumplimento de la normativa de protección de datos en un ámbito determinado, y formular unas recomendaciones que permitan a los responsables de ficheros adaptar, en su caso, su actuación a las exigencias legales.

2.1. Actuaciones derivadas de los Planes de Oficio 2001

En el ejercicio 2002 finalizaron las actuaciones inspectoras correspondientes a los Planes de Oficio desarrollados en el sector de la Banca a Distancia y en el Registro de Aceptaciones Impagadas.

2.1.1. *Plan de Oficio al Sector de la Banca a Distancia*

Durante los ejercicios de 2001 y 2002 se llevó a cabo el plan de oficio al sector de la banca a distancia del que ya se adelantaron algunas conclusiones en la Memoria del ejercicio anterior. Como resultado de dicho Plan y dentro del ejercicio de 2002, se elaboró un documento final de conclusiones y recomendaciones al sector, cuyo texto íntegro se reproduce a continuación:

Conclusiones relativas al Plan de Inspección de Oficio al Sector de la Banca a Distancia con objeto de verificar el grado de adecuación de sus ficheros de clientes y clientes potenciales a la Ley Orgánica 15/1999, de protección de datos de carácter personal

Introducción

Por acuerdo del Director de la Agencia de Protección de Datos, se procedió durante el año 2001 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, Ley 15/1999, de 13 de diciembre (LOPD) y normativa que la desarrolla.

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 el presente documento conclusiones y recomendaciones sobre algunos tratamientos de los que se ha tenido conocimiento en el transcurso de las auditorias 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 las recomendaciones sirvan al sector en su conjunto para adecuar su funcionamiento a la normativa de protección de datos.

Finalmente debe puntualizarse que el presente informe recoge 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* o CRM especializados en tratamientos complejos y masivos de la información de los usuarios. No obstante, no se ha detectado la utilización de estos sistemas para la realización de perfiles personales individualizados, sino para la obtención de datos agregados sobre el comportamiento y aceptación de los productos y servicios ofrecidos por la entidad, así como para la selección del conjunto de clientes a los que ofrecer un determinado producto o servicio.

- *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, por lo que podría incurrir en un incumplimiento del artículo 4.3 de la LOPD.

- *Respecto de las 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 todos sus datos personales 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 la entidad que puede seguir prestándole su actividad.

  En el caso de que el cliente haya solicitado además la cancelación de sus datos personales, las 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 recoja la 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, y en relación con el artículo 30 de la LOPD, 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.

En relación también con el artículo 11 de la LOPD, 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, como por ejemplo la inclusión de una casilla al efecto.

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.

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 de 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 financieras.

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, por lo que resultan adecuados dichos procedimientos al 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.

En teoría, la arquitectura de claves establecida por las entidades ofrece seguridad. No obstante, en la práctica pueden aparecer ciertas situaciones que puedan presentar algún riesgo, 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.

Se trata, en consecuencia, de establecer un equilibrio entre la consistencia del sistema de autenticación utilizado por un lado y la capacidad de asimilación del cliente por otro. En este sentido sería conveniente que las entidades facilitasen al cliente información sobre los sistemas de cifrado: sus riesgos y las formas de disminuirlos, como por ejemplo, la buena práctica de seleccionar claves que contengan letras y números, que la clave no contenga información que identifique a la persona (número de teléfono, nif, fecha de nacimiento, etc.), así como la conveniencia de cambiar las claves cada cierto tiempo. En este sentido, es muy importante la información que las entidades facilitan al cliente al respecto, comprobándose que dicha información puede ser mejorada.

Por otro lado, se han constatado también determinadas situaciones puntuales que son susceptibles de mejoras en algunas entidades y que se relacionan a continuación. Bien entendido, como se ha señalado anteriormente, que dichas situaciones no se producen acumulativamente en las entidades analizadas, sino puntualmente en unas u otras.

- Respecto de la información facilitada por la entidad, se ha encontrado una situación en la que operadores de una entidad conminaban a los clientes, durante el proceso de alta, a que seleccionasen como clave su propia fecha de nacimiento. Esta práctica introduce riesgos sobre todo cuando dicha clave no se utiliza en su conjunto sino a través de posiciones de la misma ya que, en este caso, determinadas posiciones son fácilmente predecibles.

- También, respecto de la información facilitada por las entidades, se ha constatado como en el contrato de una de ellas se afirma que las claves únicamente son conocidas por el usuario, cuando la realidad es que las claves de identificación y de autenticación, para dicha entidad, han de ser facilitadas en su totalidad, además, al operador de acceso telefónico.

- Otra situación detectada consiste en utilizar exactamente los mismos procedimientos sobre las mismas claves, incluida la de firma, para el acceso a través del operador telefónico y a través de Internet, lo que puede llevar a que dicho procedimiento no identifique de forma inequívoca y personalizada al usuario. En este sentido hay que tener en cuenta que las operaciones realizadas por los empleados de las entidades quedan registradas cuando son realizadas desde los ordenadores de la entidad, por lo que pueden depurarse fácilmente responsabilidades, no siendo así en el caso de un empleado desleal que, conociendo las claves de un cliente, le suplante desde los canales telefónicos e Internet establecidos para la comunicación entre cliente y entidad.

- En relación con el punto anterior, algunas entidades solicitan en los accesos por Internet, y cuando no es por tarjeta de claves, posiciones de la clave de autenticación y de la de firma. Esta práctica tiene sentido en los accesos a través del teléfono, ya que impide que el operador conozca las claves completas del cliente. Sin embargo, en los accesos por Internet, cuando se solicitan posiciones aleatorias de las claves y no la clave completa se introduce un factor adicional de riesgo sin que se facilite por ello la labor al cliente.

- Algunas entidades solicitan de forma reiterada los valores erróneos o no contestados por el supuesto cliente relativos a las posiciones concretas de su clave o tarjeta de claves, reiterándose dicha solicitud hasta que se facilite correctamente o se bloquee la cuenta como consecuencia de los errores acumulados. Sin embargo, no todas las entidades siguen dicha práctica, y en su lugar, y ante la situación planteada, solicitan una nueva posición aleatoria, lo que puede ser utilizado en su beneficio por quien pretenda suplantar a un cliente al conocer algunas de las posiciones de su clave o tarjeta de claves.

- Por lo general, el cliente puede cambiar las claves de autenticación y la de firma y en la mayoría de los casos incluso elegirlas. En este caso, si la elección se realiza por vía telefónica el operador conoce la clave (en los casos detectados, al menos la clave de autenticación) pese a que en el contrato entre entidad y cliente se afirma que las claves sólo son conocidas por el cliente. En estos casos seria conveniente habilitar un procedimiento que impida que el empleado conozca la totalidad de la clave.

- Otra situación detectada se produce durante el cambio de la clave cuando se realiza a través del teléfono. En estos casos, el procedimiento habitual establecido para el cambio de la clave de firma consiste en dividir la tarea entre dos operadores de grupos dis-

tintos: uno del grupo de atención general y otro del grupo de seguridad. El primero de los operadores conoce la identificación de la persona, mientras que el operador de seguridad conoce la clave elegida por el cliente, existiendo como nexo entre ambos operadores un número que ambos operadores conocen (este mecanismo se denomina *«pantalla ciega»* ya que el operador de seguridad no tiene acceso a ningún dato personal del cliente). Este mecanismo presenta el riesgo de que el acuerdo de dos operadores permitiría realizar una transferencia sin que los rastros de auditoria señalaran nada anómalo.

En relación con lo anterior, se considera que las siguientes políticas contribuyen a disminuir los riesgos existentes en las situaciones detectadas:

- Que las entidades faciliten a los clientes información acerca de la buena práctica de gestión de claves: como la conveniencia de seleccionar claves que contengan letras y números y que preferiblemente no tengan una relación directa con la persona (número de teléfono, nif, fecha de nacimiento, etc.), la idoneidad de cambiar las claves con cierta frecuencia, y en general todos aquellos aspectos que contribuyan a preservar la confidencialidad de las mismas.

- Que los operadores del canal telefónico no recaben claves completas del cliente si éste se encuentra identificado para ellos, así como, que se diferencien los accesos a través de los canales telefónico e Internet de forma que no se utilicen los mismos procedimientos de acceso sobre las mismas claves. Todo ello, con el fin de evitar que a través de empleados desleales se pueda producir una suplantación del cliente sin que de ello quede constancia en los ficheros de la entidad.

- Que se soliciten de forma reiterada los valores erróneos o no contestados por el supuesto cliente relativos a las posiciones concretas de su clave o tarjeta de claves, reiterándose dicha solicitud hasta que se facilite correctamente o se bloquee la cuenta como consecuencia de los errores acumulados. Con ello se disminuye el riesgo de que un tercero, con conocimiento sobre una parte de la clave, pueda realizar un acceso no autorizado.

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, 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 per-

sonales 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, se facilitan determinados datos personales a partir únicamente del correspondiente NIF de la persona, lo que permite conocer a cualquiera si una persona es o no cliente de dicha entidad, y en su caso, sus datos identificativos.

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 en el apartado 2.3, 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 recojan dichos contratos 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 de la LOPD 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 decisio-

nes 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 con base en 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 mailing 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 un carácter 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 telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.».*

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 el fichero, 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 obligaciones dinerarias, comunicando al fichero común los impagos producidos y consultando en el fichero común 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 en el apartado 2.3, 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.

Recomendaciones a las entidades de Banca a Distancia

A tenor de lo expuesto, y en atención al resultado de las actuaciones practicadas por parte de la Inspección de Datos, se han observado ciertas deficiencias en los Sistemas de Información de entidades que se dedican a la denominada banca a distancia en relación al cumplimiento de las prescripciones de la Ley Orgánica 15/1999 y su normativa de desarrollo, cuya subsanación supondría una sustancial mejora en el acatamiento del citado marco normativo.

Por lo tanto, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga en 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 las entidades de este sector, al objeto de adecuar los tratamientos automatizados que realizan a los principios de la normativa vigente en materia de protección de datos de carácter personal.

Primera: En relación con la calidad de los datos personales (artículo 4 de la LOPD)

Respecto de la incorporación a los propios sistemas de la entidad de datos procedentes de ficheros de incumplimiento de obligaciones dinerarias constituidos al amparo del artículo 29 de la LOPD, debe distinguirse según que la información se refiera o no a clientes. Respecto de los clientes de la entidad financiera los datos obtenidos de ficheros regulados en el artículo 29 de la LOPD no resulta necesario que sean actualizados si se mantienen en ficheros que, no siendo de morosidad, incluyan otras informaciones personales del cliente. Por el contrario, en el caso de personas que no son clientes de la entidad o, en el de clientes de la entidad cuyos datos se incorporan a ficheros de solvencia patrimonial y crédito, se recomienda que, o bien se proceda a la cancelación de la citada información una vez se haya tramitado la solicitud de crédito, o en su defecto se habiliten los controles y procedimientos pertinentes para que dicha información sea exacta y puesta al día de forma que responda con veracidad a la situación actual del afectado tal y como establece el artículo 4.3 de la LOPD.

En relación a la cancelación de los datos personales cabe señalar que si bien existen obligaciones legales de mantener ciertos conjuntos de datos durante determinados períodos de tiempo (cinco años para finalidad fiscal, etc.), no debe extrapolarse dicha obligación a la totalidad de los datos que se tengan de una persona, como por ejemplo los datos de *marketing*, por lo que aquellos datos cuyo mantenimiento no cuente con amparo legal, deberán ser suprimidos, no siendo suficiente en este caso el bloqueo de los mismos en consonancia con lo establecido en el artículo 16.3 de la LOPD.

Respecto del proceso de alta como cliente, debiera establecerse un plazo razonable desde la apertura de dicho proceso, transcurrido el cual, se cancele toda la información de aquellos solicitantes que no hubieren llegado a completar su alta.

Segunda: En relación con el derecho de información en la recogida de datos y el consentimiento (artículos 5 y 6 de la LOPD)

El artículo 5 de la LOPD establece que *«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».*

La información facilitada durante la recogida de los datos es la base del consentimiento inequívoco requerido, como principio general, por el artículo 6 de la LOPD. Si bien las enti-

dades analizadas proporcionan información, no siempre ésta recoge todos los aspectos contemplados en la normativa de protección de datos.

Por lo tanto, deberá establecerse un sistema que contraste la coherencia e integridad de la información facilitada a través de los diferentes medios utilizados por la entidad. De hecho, sería deseable que independientemente del medio consultado, la información fuese la misma. Dicha información deberá incluirse de forma obligatoria como parte integrante del proceso de recogida de datos personales, de forma que resulte fácilmente accesible para el usuario.

De no unificarse la información y en tanto en cuanto se faciliten informaciones distintas según el medio utilizado para recabar los datos, las entidades deberán adoptar las medidas necesarias para evitar en cada caso los tratamientos de datos o cesiones de los que no se hubiere informado a cada afectado.

Deberá especificarse qué información de la recabada se considera obligatoria y que información se considera voluntaria, siendo declarada como obligatoria la que resulte adecuada pertinente y no excesiva para la prestación del servicio contratado. En el caso de recabar información adicional voluntaria deberá especificarse la finalidad de la misma.

Deberá también informarse al cliente de los tratamientos que tengan como finalidad la realización de segmentaciones o perfiles de clientes con fines comerciales, así como establecer un procedimiento fácil y directo que permita ejercer la oposición a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

Respecto de los servicios de *agregadores financieros* seria conveniente que la entidad prestataria del servicio se limitara exclusivamente a presentar la información de las posiciones de los usuarios en las entidades previamente establecidas, procediendo a cancelar dicha información en cuanto deje de ser necesaria. Cualquier otro tratamiento que la entidad prestataria del servicio desee realizar deberá contar con el consentimiento previo e informado del usuario ofreciendo siempre la posibilidad de oponerse al mismo mediante un procedimiento fácil y directo como la inclusión de una casilla al efecto.

Tercera: 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 y a la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

De acuerdo a lo establecido en el citado Reglamento, las entidades deberán cumplir las medidas de seguridad aplicables a cada uno de los ficheros en función de su clasificación como ficheros de nivel básico y medio.

Respecto de las medidas de seguridad y especialmente en relación con el artículo 18 del citado Reglamento, se recomienda que se diseñen los mecanismos de identificación establecidos de forma que garanticen que la identificación del usuario que intenta acceder al sistema es inequívoca y personalizada, dado que se han detectado situaciones que aunque por si solas y de forma aislada no representan fallos de seguridad sí que pueden contribuir, ya sea por acumulación de varias o por combinación con otros factores, a que los mecanismos de identificación no garanticen dicha identificación en los términos establecidos en el citado artículo.

Cuarta: En relación con el deber de secreto (artículo 10 de la LOPD)

Se recomienda incluir en los contratos de trabajo cláusulas relativas al deber de secreto respecto de los datos personales a los que tienen acceso los empleados como consecuencia de su actividad, ya sean los propios empleados de la entidad como los empleados de las empresas prestatarias de servicios para la entidad con acceso a los datos personales de los clientes.

Se recomienda también que las páginas web de acceso a los servicios se diseñen de tal manera que no proporcionen al usuario más datos personales que los introducidos por el propio usuario, hasta que éste no haya superado con éxito los controles de identificación y autenticación.

Quinta: En relación con las 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 legítimas 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».*

Si bien las entidades analizadas han manifestado no realizar cesiones de datos a terceros, lo cierto es que en la información que algunas de ellas facilitan a los clientes figuran cláusulas tipo que informan de la posibilidad de efectuar cesiones a *«empresas del grupo»* para *«la oferta y contratación de otros productos y servicios»*, sin especificar ni las empresas ni los sectores de actividad a que pertenezcan las mismas y sin que éstos sectores puedan deducirse en base a la naturaleza de los productos y servicios que pudieran ofertarse.

En relación con cláusulas como la apuntada cabe señalar que su contenido resultaría insuficiente, ya que no permite conocer la finalidad a que se destinarían 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. En definitiva, y como establece el artículo 4.1 de la LOPD, las finalidades para las que se recaben datos han de ser determinadas, explícitas y legítimas.

Por lo expuesto, en caso de que se prevea la realización de cesiones a otras empresas deberá recabarse con carácter previo a la cesión el correspondiente consentimiento en los términos establecidos en la Ley. Igualmente, la cláusula por la que se informa de la posibilidad de la cesión de los datos personales a terceros deberá recoger un procedimiento que permita al interesado expresar su oposición, como por ejemplo la inclusión de una casilla al efecto.

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

Se ha detectado en todas las entidades auditadas la existencia de contratos con terceros para la prestación de servicios que conllevan el acceso a determinados ficheros por parte de las terceras empresas, prestadoras de servicios.

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 responsa-*

ble del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.»

Como ya se ha mencionado en las conclusiones, 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 recojan dichos contratos lo estipulado en el artículo 12 de la LOPD, si bien se han detectado algunos contratos en los que no se recogen todos los requisitos exigidos en el citado artículo.

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 contratos de prestación de servicios establecidos con terceros deben adecuarse a lo previsto en el artículo 12 de la LOPD.

A estos efectos, se recomienda que en las prestaciones de servicios que tengan por objeto la realización de un tratamiento de datos por parte de un tercero, la entidad debe tener en cuenta, como responsable del fichero, lo siguiente:

a) 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 la 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.

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

   Por otra parte, aunque en la inspección practicada no se ha detectado que se lleven a cabo subcontrataciones, la experiencia ha demostrado la frecuencia con que las empresas prestadoras de servicios a terceros suelen subcontratar con otras empresas parte del servicio a prestar.

   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 prestadora del servicio subcontrate a su vez esta segunda actividad con otra empresa, a menos que la prestadora actúe en nombre y por cuenta del responsable del fichero.

Séptima: En relación con los datos procedentes de fuentes accesibles al público con fines de publicidad y prospección comercial (artículo 28 de la LOPD)

En este sentido, en el caso de datos procedentes de fuentes accesibles al público, deberán establecerse los controles pertinentes para garantizar la actualización de los datos, de forma que se tenga en cuenta el carácter temporal de la fuente de acceso público, en consonancia con lo estipulado en el artículo 28.3 de la LOPD.

Adicionalmente, las entidades que habiendo constituido un fichero a partir de datos obtenidos de fuentes accesibles al público con fines de publicidad y prospección comercial y que procedan a incorporar datos adicionales, no procedentes de fuentes accesibles al público, habrán de tener en cuenta los requerimientos establecidos en la normativa de protección de datos para el tratamiento de dichos datos y, en particular, la necesidad de contar con el consentimiento informado del afectado.

Octava: En relación con los tratamientos con fines de publicidad y de prospección comercial (artículo 30 de la LOPD)

En los casos en que se vayan a tratar datos personales para la promoción comercial de productos y servicios de entidades distintas de aquella con la que se ha establecido una relación contractual, en el momento en que se recaben datos personales deberá informarse de las finalidades específicas para las que van a ser utilizados tales datos, debiendo habilitarse un mecanismo que permita al usuario, en ese momento, poder dejar constancia de su oposición a dicho tratamiento, como por ejemplo la inclusión de una casilla al efecto.

2.1.2. *Recomendaciones relacionadas con el Registro de Aceptaciones Impagadas (R.A.I.)*

Dentro de los Planes Sectoriales de Oficio que la Agencia de Protección de Datos lleva a cabo con carácter anual, durante el año 2001 se procedió a realizar un Plan de Inspección al fichero RAI (Registro de Aceptaciones Impagadas), cuyo responsable es el CENTRO DE COOPERACIÓN INTERBANCARIA, en (adelante CCI) del que se dio amplia información en la Memoria correspondiente al año 2001.

Como resultado de las actuaciones practicadas por la Inspección de Datos, se observaron ciertas deficiencias en los sistemas de información que afectaban al fichero RAI en relación al cumplimiento de las prescripciones de la Ley Orgánica 15/1999. Por ello, en el año 2002 se dictaron las RECOMENDACIONES, que a continuación se transcriben las cuales deberían ser observadas por las entidades CCI, como responsable del fichero y por CTI, como encargado del tratamiento, al objeto de adecuar los tratamientos a los principios de protección de datos.

RECOMENDACIONES

A tenor de lo expuesto y como resultado de las actuaciones practicadas por la Inspección de Datos, se han observado ciertas deficiencias en los Sistemas de Información que afectan al fichero RAI en relación al cumplimiento de las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre, cuya subsanación supondría su adecuación a las exigencias de la citada Ley Orgánica y de la normativa que la desarrolla.

Por lo tanto, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga 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 las entidades CCI y CTI, al objeto de adecuar plenamente los tratamientos automatizados que realizan a los principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Recomendación primera: Calidad de datos

Exactitud de los datos

El artículo 4.3 de la Ley Orgánica 15/1999, relativo a la *calidad de los datos*, indica que *«los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado».*

El fichero RAI 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.

A este respecto, CCI debe establecer un sistema de forma que los datos incluidos en el fichero RAI *respondan con veracidad a la situación actual del afectado*, no pudiendo incluirse en el fichero común ningún dato personal relativo a deudas inexistentes o ya saldadas.

Por su parte, las entidades informantes sólo podrán incorporar información al fichero RAI de conformidad con el artículo 29 de la LOPD, es decir, cuando ostenten la condición de acreedor o puedan acreditar que actúan por cuenta o interés de aquél.

Cancelación de datos

La Ley Orgánica 15/1999, en el artículo 4.5 y bajo el epígrafe «calidad de datos», consagra el principio de conservación limitada de los datos al disponer: *«los datos de carácter per-*

sonal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados de 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».

Como ayuda para la gestión del fichero RAI, las entidades CCI y CTI mantienen diversos ficheros que contienen datos de forma permanente en algunos casos y que en ocasiones podrían contener datos relativos a personas físicas que nunca han formado parte del citado fichero. Así:

a) CCI dispone de un fichero creado en 1996 para gestionar el ejercicio de los derechos de los afectados, del que no se ha borrado ningún registro desde su creación. Es de destacar que en este fichero se pueden encontrar datos relativos a personas físicas que no hayan formado parte en ningún momento del fichero RAI.

   En virtud de las prescripciones legales transcritas, respecto al fichero reseñado en este apartado, CCI podrá mantener los datos relativos a personas físicas identificadas, únicamente durante el plazo de prescripción de las acciones legales. No obstante el citado fichero deberá ser notificado e inscrito en el Registro General de Protección de Datos.

b) CTI mantiene dos ficheros Históricos que contienen de forma permanente desde 1994 la siguiente información:

   El primero de ellos contiene datos relativos a deudas que han sido dadas de baja en el RAI por las entidades informantes.

   El segundo fichero contiene datos relativos a deudas que han sido dadas de baja en el RAI por tiempo de permanencia en dicho fichero superior a 30 meses.

   Respecto a los ficheros reseñados en este apartado, el artículo 29.4 de la LOPD especifica que «Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la

situación actual de aquéllos». Por tanto los datos no deben permanecer en estos ficheros por un período superior a los seis años especificados en el citado artículo de la LOPD.

Los citados ficheros no pueden calificarse como de información sobre solvencia patrimonial y crédito al no ser accesibles por terceras entidades. En consecuencia, para adaptarse a las exigencias de la LOPD deberán ser notificados e inscritos en el Registro General de Protección de Datos debiendo procederse al bloqueo de los datos contenidos en ellos en los términos del artículo 16 de la LOPD.

c) CTI gestiona un fichero que utiliza para realizar la facturación a las entidades que consultan el RAI. Los datos incluidos en dicho fichero se mantienen en línea durante el año en curso, y al finalizar el mismo son traspasados a otro fichero histórico con la misma estructura que el primero, donde se conservan durante un año más.

   El citado fichero puede contener datos relativos a las personas físicas que han sido consultadas por las entidades (al menos nombre y apellidos y, en ocasiones, DNI y provincia) aunque dichas personas no hayan figurado en ningún momento en el fichero RAI.

   Respecto al fichero reseñado en este apartado, CTI deberá proceder a comunicar a los afectados que ejerzan el derecho de acceso, la información contenida en dicho fichero en los términos del artículo 15 de la LOPD. Así mismo, el fichero deberá ser notificado para su inscripción en el Registro General de Protección de Datos.

   Cuando concurran las circunstancias previstas en el artículo 4.5 de la LOPD, deberá procederse al bloqueo de los datos conforme al artículo 16 de la misma norma.

Recomendación segunda: Deber de secreto

El artículo 10 de la LOPD relativo al *Deber de secreto*, especifica que *«El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo»*.

CTI 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, no existe ningún documento por el cual las personas que prestan sus servicios en CCI queden obligadas al secreto profesional sobre los datos a los que acceden en el desempeño de sus funciones, por lo que dichas personas deberán firmar un compromiso de confidencialidad con CCI que contemple lo especificado en el citado artículo 10 de la LOPD.

Recomendación tercera: Comunicación de datos

El artículo 29.3 de la Ley Orgánica 15/1999, relativo a la *Prestación de servicios de información sobre solvencia patrimonial y crédito*, establece que *«... cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos»*.

A fecha de la inspección realizada, existen dos modalidades de acceso al fichero RAI:

a) Acceso a la copia del fichero RAI disponible en cada entidad presentadora / receptora.
b) Acceso *on-line* al fichero completo desde entidades informantes.

A la vista de la modalidad de acceso a) se desprende que CCI no está en disposición de informar completamente al interesado de los accesos a sus datos realizados durante los últimos seis meses, ni del nombre y dirección de la persona o entidad a quien se hayan revelado los datos, ya que las consultas efectuadas a las copias del fichero RAI son desconocidas por CCI. Tampoco conoce CCI el destino dado a dichas copias por las entidades presentadoras / receptoras, aunque supuestamente estas entidades lo ponen a disposición de las entidades informantes a las cuales representan en el sistema. En consecuencia, deberá comunicar la relación de tales entidades.

Respecto a la modalidad de acceso b), ante la consulta por nombre y apellidos realizada por una entidad, CTI responde con las diversas posibilidades existentes en el fichero RAI coincidentes con la consulta efectuada, no guardando CTI datos de la persona concreta que finalmente la entidad ha consultado. Por tanto, en este caso, al no conocer exactamente CTI la persona consultada, tampoco puede ofrecer las evaluaciones realizadas sobre la misma en los últimos seis meses.

A la vista de los hechos descritos y de conformidad con la prescripción legal indicada, CCI deberá, como responsable del fichero, establecer un sistema que garantice, respecto de la modalidad de acceso b), el derecho de los afectados a conocer las evaluaciones que sobre ellos se hayan comunicado en los últimos seis meses, así como el nombre y dirección de la persona o entidad a quien se hayan revelado sus datos.

Recomendación cuarta: Acceso a los datos por cuenta de terceros

En el artículo 12.2 de la LOPD se especifica 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 está obligado a implementar».

Entre CCI y CTI existe un contrato de prestación de servicios de fecha 31/1/95, por el cual CTI se compromete a realizar la gestión informática del fichero RAI y a instrumentar las contestaciones a las solicitudes de información de los interesados.

En dicho contrato no se hace ninguna referencia expresa a 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 y que no los comunicará, ni siquiera para su conservación, a otras personas. Tampoco se estipulan las medidas de seguridad a que se refiere el artículo 9 de la LOPD y que CTI está obligada a implementar.

Por lo tanto, el contrato suscrito entre CCI y CTI deberá actualizarse a fin de que contemple todos los aspectos indicados en el citado artículo 12.2 de la LOPD.

Recomendación quinta: Derechos de acceso, rectificación y cancelación

El artículo 15.1 de la LOPD especifica que *«El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos».*

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 los ficheros Históricos en los que se graban los registros borrados del RAI o en el fichero de atención de los derechos, en el que se pueden encontrar datos de nombre, apellidos y domicilio relativos a personas físicas cuyos datos nunca hayan estado incluidos en RAI.

Tampoco se informa de la posible existencia de datos del afectado en el fichero utilizado para realizar la facturación a las entidades que consultan on-line el fichero RAI, en el que también se pueden encontrar datos de personas físicas cuyos datos nunca hayan estado incluidos en el RAI.

En consecuencia, conforme a lo especificado en la LOPD, ante el ejercicio de los derechos de los afectados, CCI debe ofrecerles la información completa que de ellos se dispone consultando para ello todos sus ficheros que contengan datos de carácter personal.

Recomendación sexta: Registro General de Protección de Datos

El artículo 26.1 de la LOPD especifica que *«Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos»*.

A este respecto, únicamente se encuentra inscrito en el Registro General de Protección de Datos el fichero RAI.

Sin embargo, no se encuentra inscrito en dicho Registro el fichero utilizado para gestionar y controlar la atención de los derechos de los afectados. Tampoco se encuentra inscrito el fichero de facturación a entidades por las consultas realizadas, ni los ficheros Históricos que contienen los datos borrados del RAI.

Por estas razones, y a tenor de lo especificado por la LOPD, tanto CCI como CTI deberán proceder a la inscripción registral de aquellos ficheros de los que sean responsables.

Como consecuencia de las Recomendaciones de la Agencia de Protección de Datos que se acaban de transcribir, CCI ha elaborado un plan de actualización de funcionamiento del fichero RAI, que incluye una serie de medidas que se implantarán a lo largo del año 2003.

Dichas medidas han sido plasmadas en el documento de fecha 20/11/02 denominado Normas de Funcionamiento del RAI que ha sido presentado ante la Agencia, y del que se pueden destacar los siguientes aspectos:

- Las entidades adheridas al sistema únicamente podrán consultar el fichero RAI en la modalidad on-line.

- La incorporación en los documentos contractuales de cláusulas que autoricen a actuar por cuenta e interés del acreedor, así como la obligatoriedad por parte de éste de informar del pago extrabancario.

- Los datos del acreedor figurarán únicamente a efectos de la remisión de la notificación de inclusión al afectado y de la atención ante el ejercicio de sus derechos. Sin embargo este dato no se encontrará disponible en las consultas realizadas por las entidades.

- En la información incluida en el RAI figurará necesariamente el NIF del deudor.

- Entrará en funcionamiento la notificación al deudor del impago producido, en nombre de la entidad de crédito donde se ha de realizar el pago, reclamando el pago en nombre del acreedor y avisando de la inclusión de sus datos en el RAI en caso de no realizarse el pago.»

2.2. Planes Sectoriales de Oficio 2002

En el año 2002 la Agencia ha seguido impulsando la realización de Planes Sectoriales de Oficio.

Las actuaciones realizadas se han referido al tratamiento de datos personales en Concursos, Juegos y Sorteos de Televisión, así como al Proyecto de Censos de Población y Viviendas 2001, del Instituto Nacional de Estadística.

2.2.1. *Concursos, Juegos y Sorteos de Televisión*

La inspección sectorial sobre el tratamiento de datos en Concursos, Juegos y Sorteos de Televisión desarrollada en el año 2002 dio lugar a la adopción por el Director de la Agencia del documento de CONCLUSIONES Y RECOMENDACIONES que se transcribe a continuación:

La Agencia de Protección de Datos tiene conocimiento de que últimamente han proliferado en los medios españoles un gran número de formatos televisivos a través de los cuales se recaba la participación pública, lo que en ocasiones puede suponer la recogida indiscriminada de datos personales de la audiencia. Este tipo de actividades deberían siempre llevar asociado el establecimiento, por parte de todas las entidades implicadas, de las garantías adecuadas que permitan asegurar que el tratamiento de tales datos no menoscaba en el ciudadano el ejercicio de un derecho fundamental como es el de la protección de sus datos de carácter personal, tal y como lo consagran las sentencias del Tribunal Constitucional 290/2000 y 292/2000, ambas de 30 de noviembre, y la Carta de los Derechos Fundamentales de la Unión Europea, proclamada por los Jefes de Estado y de Gobierno de la Unión Europea en Niza el 7 de diciembre de 2000.

Esta Agencia vela por el cumplimiento de la Ley en relación con la doctrina mantenida por el Alto Tribunal, cuando reconoce *«el poder de control del ciudadano sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»*, y cuando considera que tal derecho *«no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal»*.

Así, haciendo uso de las funciones atribuidas a la Agencia por la Ley Orgánica 15/1999, y en consonancia con el carácter preventivo de sus actuaciones, es objetivo de este organismo contribuir a lograr que las actividades que giran alrededor de la realización de los citados programas de televisión se desarrollen de acuerdo con los principios establecidos por la Ley Orgánica, identificando para ello cuáles son las deficiencias que deberían subsanar las entidades implicadas, con objeto de mejor salvaguardar los derechos de los ciudadanos en relación con el tratamiento de sus datos de carácter personal.

A este respecto, y como complemento a las actividades desarrolladas por la *«Ponencia de estudio de los derechos de concursantes y audiencia en relación con concursos, juegos y apuestas»*, constituida en el seno de la Comisión de la Sociedad de la Información y del Conocimiento del Senado, en el mes de febrero el Director de la Agencia de Protección de Datos asumió el compromiso de realizar las oportunas actuaciones inspectoras con el objetivo de determinar la adecuación a la legislación vigente de los ficheros constituidos con datos de personas que intervienen en programas de televisión, siempre que su intervención suponga de alguna forma la participación en concursos, juegos o sorteos. En este sentido, no se han incluido en el presente análisis los ficheros en los que tan sólo se almacenan datos de las personas que intervienen en los programas televisivos para exponer sus experiencias u opiniones, cuando esa intervención no supone la participación en un concurso, juego o sorteo.

Al iniciarse el análisis, una primera observación de la información que constaba en el Registro General de Protección de Datos permitió obtener algunas líneas de investigación:

- La inscripción de ficheros con datos de concursantes por parte de las compañías emisoras de televisión revelaba su intervención en la producción de este tipo de programas, pero también reflejaba la obtención por parte de algunas de estas compañías de los datos recabados por otras (canales temáticos o productoras).

- Los ficheros analizados eran generalmente relativos a la participación en concursos, incluyéndose datos referidos tanto a personas que intervienen de forma presencial como a aquellas otras que participan por vía postal, telefónica (incluyendo el envío de mensajes cortos sms) o a través de Internet. Destacaban también aquellos concursos en los que para la selección de los concursantes se realiza un proceso de «*casting*» y no un simple sorteo, ya que en ese proceso pueden colaborar otras entidades.

- Junto con los programas concebidos fundamentalmente como concursos o juegos de participación de la audiencia, existen otros más generales, de los que se habían declarado ficheros con datos de personas, generalmente niños, asociados para formar parte de clubes promotores de actividades diversas (culturales, deportivas, ocio), los cuales pueden utilizar los datos de los miembros o socios para el envío de publicidad de las entidades patrocinadoras.

- Se consideraron también otros programas que no eran siempre concursos pero que, con el reclamo de un premio a sortear entre los participantes, sondeaban la opinión de la audiencia al respecto de cuestiones diversas, obteniendo para ello sus datos personales (asociados, por tanto, a la opinión manifestada). Algunos de éstos utilizan la vía de los mensajes cortos sms para obtener estas opiniones.

- En la inscripción de los ficheros relacionados con determinados concursos que implican la convivencia de los participantes se hacía constar que contienen datos de los que la LOPD considera especialmente protegidos, en particular, relativos a la salud y vida sexual.

Por otra parte, entre los antecedentes que constan en la agencia figuran también algunos procedimientos sancionadores iniciados como consecuencia de la realización de las correspondientes actuaciones de inspección, las cuales habían revelado la participación de múltiples entidades en ciertos procesos de selección de concursantes, ocasionando el acceso a datos personales por cuenta de terceros sin las debidas garantías y favoreciendo que, en algún caso, por la espectacular relevancia de que determinados concursos llegan a gozar, tales datos pudieran filtrarse a través de medios públicos.

De la misma forma, la Inspección tenía conocimiento de determinadas compañías cuyo objeto social se centra en la recopilación de datos personales de participantes en diversos concursos televisivos y en su posterior tratamiento con fines comerciales, para lo cual se establecen ciertas relaciones con las compañías (productoras o televisiones) que se han encargado de recabar los datos.

Actuaciones realizadas

A la hora de delimitar el colectivo de entidades que iban a ser objeto de análisis por parte de la inspección, se han tenido en cuenta no sólo aquéllas que se han declarado, a través del Registro General de Protección de Datos, como responsables de los ficheros (las televisiones y las productoras de televisión), sino también otras entidades que pueden participar en el tratamiento de datos personales, generalmente en calidad de «*encargado de tratamiento*» o cesionario. Así, dentro del presente plan se ha realizado visita de inspección a un total de 19 entidades que participan de una u otra forma en la realización de los programas que son objeto de análisis. Entre ellas figuran 5 compañías que prestan el servicio público de televisión, tres de ellas (con ámbito nacional) titulares de una concesión administrativa y las otras dos dependientes de entidades con naturaleza jurídica pública (una nacional y otra de ámbito autonómico), las cuales también han sido inspeccionadas. Así mismo, se han visitado 4 productoras de programas televisivos, 5 compañías especializadas en servicios de valor añadido (audiotex y recepción de mensajes cortos sms) y otras 3 compañías que prestan servicios diversos.

Resultados obtenidos

Se ha podido constatar que una de las principales vías de obtención de datos personales relativos a la audiencia de televisión (TV) son las líneas telefónicas 906. Los servicios audiotex que se prestan a través de estas líneas están regulados en la *Orden PRE/361/2002, de 14 de febrero, del Ministerio de la Presidencia, de desarrollo, en lo relativo a los derechos de los usuarios y a los servicios de tarificación adicional, del título IV del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones.* En particular, el artículo 18.5 establece que los prestadores de servicios «*deberán elaborar un plan de publicidad para garantizar una adecuada y suficiente información al público sobre el funcionamiento de estos servicios*» y, entre otras cuestiones, prevé la obligatoriedad de informar telefónicamente acerca del precio máximo por minuto de llamada en el momento de iniciarse la comunicación.

Las líneas de tarificación adicional son atendidas por compañías especializadas en la prestación de servicios de audiotex, que son las titulares de la línea telefónica y que, según se ha podido comprobar, almacenan en sus propios servidores las grabaciones de audio con los datos facilitados telefónicamente. A este respecto, también se ha verificado que el almacenamiento de las grabaciones no está indexado por el número de la línea llamante, dato este que no queda registrado. La locución que escucha la persona que realiza la llamada guía a ésta para que facilite sus datos, los cuales suelen consistir en: nombre y apellidos, número telefónico de contacto, edad y población de residencia, aunque, en ocasiones, también se recaban datos sobre domicilio, estado civil y número de D.N.I..

Se trata de conseguir por esta vía que la audiencia participe activamente en los programas de televisión, de tal forma que las votaciones de los televidentes decidan parcialmente sobre el desarrollo del programa. Estos programas suelen tener formato de magazines, variedades o concursos y utilizan como reclamo el sorteo de un premio entre los participantes. Generalmente los datos personales así obtenidos no llegan a transcribirse en formato texto, siendo las grabaciones de audio destruidas por la compañía de audiotex, una vez que se realiza el correspondiente sorteo. Los servicios son generalmente contratados por la cadena de televisión que emite el programa, la cual se reparte con la titular de la línea 906 los beneficios obtenidos a través de la facturación de la compañía telefónica.

Una práctica muy extendida en el sector de audiotex consiste en repartir el tráfico de llamadas en situaciones de congestión de la red telefónica. Así, cuando una determinada línea se satura por la gran afluencia de llamadas recibidas, lo que suele ocurrir cuando se convoca puntualmente a la audiencia a realizar sus votaciones en un corto espacio de tiempo, la compañía telefónica desvía las llamadas entrantes hacia otras líneas cuya titularidad corresponde a distintas compañías de audiotex. Para ello sólo es preciso que previamente la titular de la línea que se desviará lo solicite a la compañía telefónica y que las compa-

ñías interesadas en recibir los desvíos notifiquen también a la compañía telefónica su aceptación. De esta forma, los datos personales recabados en un determinado sorteo se almacenan en los distintos sistemas informáticos utilizados por las respectivas compañías que reciben las llamadas, aunque en algunos casos estas llamadas ni siquiera lleguen a intervenir en el sorteo que se celebra.

Las líneas de tarificación adicional son también utilizadas como vía para la selección de concursantes o «*casting*». Las labores de recepción de llamadas a líneas 906 son encargadas generalmente por la productora del programa a la compañía de audiotex titular de la línea, aunque en algún caso se ha observado que la contratación la realiza la cadena de televisión que emite el programa. En general, el procedimiento seguido es el mismo que el descrito para los sorteos, aunque en estos casos los datos personales almacenados en forma de grabaciones de audio son posteriormente transcritos en formato texto por otra compañía especializada en labores de grabación informática. Los ficheros así obtenidos se entregan a la productora del concurso, que los utiliza como base para contactar telefónicamente con los interesados y convocarles, en algunos casos, a sucesivas pruebas de aptitud antes de la selección final.

Se ha detectado, sin embargo, algún caso en que el establecimiento de la línea telefónica parece responder tan sólo a un interés promocional o incluso económico, por la obtención de ingresos adicionales. No parece justificado que se recabasen datos personales de más de 4.000 participantes en ese supuesto «*casting telefónico*» y que tales datos fueran transcritos en formato de texto, pero luego no fuesen utilizados como base para la selección de concursantes, la cual se realizó a partir de los datos facilitados personalmente por los interesados en el momento de presentarse a las pruebas de aptitud. Resulta significativo, por otra parte, que en este caso la contratación de los servicios de audiotex fue realizada no por la productora sino por la cadena de televisión que emitiría el concurso, la cual recibió así parte de los beneficios obtenidos por la facturación telefónica. Es relevante además que esta misma cadena ya había comercializado en otras ocasiones datos personales de concursantes.

Otra de las vías más utilizadas para recabar la participación de la audiencia en sorteos es el envío de mensajes cortos (SMS) a través de telefonía móvil. Al igual que con los servicios de audiotex, es generalmente la cadena de televisión la que contrata estos servicios con la compañía titular de un número corto de los denominados «*premium*» (de cuatro cifras), que a su vez ha suscrito contrato con las tres operadoras de telefonía móvil que actualmente disponen de licencia en nuestro país. De esta forma cualquier usuario (sin importar la compañía que le presta los servicios de telefonía) puede remitir mensajes cortos desde su terminal móvil al citado número, siendo recibidos en la «*plataforma de mensajería*» de la propia titular del número, donde quedan almacenados indexados en función del número telefónico remitente.

Esta misma vía se ha utilizado también en alguna ocasión como alternativa para recabar datos de los interesados en participar en el «*casting*» de un concurso. En este caso los servicios son contratados por la productora del programa, que recibe en soporte informático el fichero que se constituye con los datos directamente automatizados por los propios interesados, sin necesidad de que medie una labor de transcripción. Evidentemente, el fichero así constituido posee una información más detallada acerca de las personas que han realizado las llamadas, pues contiene no sólo el número del teléfono móvil llamante sino también otros datos (nombre, provincia, edad) que permiten una mejor identificación del candidato.

En otro orden de cosas, Internet ha sido la vía elegida por la productora de un concurso musical para recabar un extenso currículum (nombre y apellidos, D.N.I., dirección completa, sexo, fecha de nacimiento, número de teléfono, dirección electrónica, características físicas, estudios, profesión, disponibilidad, experiencia televisiva, opiniones y preferencias musicales) de más de 12.000 interesados en participar en un proceso de selección de presentadores del canal temático asociado al citado formato televisivo. Estos datos sirvieron posteriormente de base para elegir y convocar a los candidatos más idóneos.

En lo relativo a la celebración de los sorteos, generalmente interviene un notario, aunque no siempre de la misma forma. Cuando la participación tiene lugar a través de una línea 906, el notario suele personarse en el lugar en que se han almacenado las grabaciones de audio (que, como ya se ha mencionado, puede ser cada uno de los servidores de las compañías que reciben las llamadas) y el sistema informático facilita «aleatoriamente» una relación de posibles ganadores, de la que el notario extrae al elegido. Cuando la participación tiene lugar a través de mensajería móvil, la compañía de servicios remite al notario un soporte informático conteniendo el texto íntegro de los mensajes recibidos y el número de teléfono remitente. Este soporte es posteriormente devuelto a la compañía de servicios para su custodia.

Finalmente, dentro de las iniciativas que tienen mayor implantación en las televisiones (tanto públicas como privadas), cabe citar la organización de programas orientados al público infantil, que llevan asociada la creación de un club de socios cuyos fines son la promoción de actividades culturales y de ocio, con la consiguiente celebración de sorteos y concursos entre los miembros del club. Generalmente la inscripción en el club puede realizarse por correo postal, a través de Internet o a través de cupones que aparecen en publicaciones escritas. Se ha observado que, en ocasiones, los datos del socio se recaban con la intención de ser utilizados con fines comerciales.

Conclusiones generales

A continuación, se analiza, desde el punto de vista de la protección de datos, el cumplimiento de cada uno de los principios legales respecto de las actividades que realizan las compañías inspeccionadas.

Información facilitada en la recogida de datos

Quizá uno de los incumplimientos más generalizados de la LOPD que se han detectado consiste en la incompleta información que se facilita al ciudadano en el momento de recabar sus datos personales. Así, las locuciones utilizadas en los sistemas audiotex no incluyen en muchos casos referencias a los extremos previstos en el apartado 1 del artículo 5 de la Ley Orgánica. De esta forma, las personas que facilitan sus datos al sistema automático no tienen conocimiento del destino final que se dará a los mismos, tanto si participan en un sorteo como si lo hacen en un proceso de selección de concursantes.

A este respecto, hay que señalar que el hecho de grabar la voz de los interesados en el momento de facilitar sus datos personales ya constituye un tratamiento de los mismos. En este sentido, se ha observado que tales grabaciones se almacenan de forma automatizada constituyendo un conjunto organizado en los mismos términos en que el artículo 3 de la LOPD define el término «*fichero*», es decir, «*cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*». A esta consideración se añade el hecho de que cuando los datos se recaban en el seno de un «*casting*» generalmente se transcriben luego sobre ficheros convencionales de texto, ya sea mediante métodos automáticos de reconocimiento de voz o con intervención humana.

De la misma forma, puede decirse que los mensajes cortos remitidos por teléfono móvil, que se almacenan junto con el número llamante, constituyen en sí mismos datos personales, de acuerdo con la definición incluida en la LOPD, que comprende «*cualquier información concerniente a personas físicas identificadas o identificables*». Así, el mero hecho de disponer de ese número telefónico permitiría al destinatario del mensaje determinar quién ha manifestado una determinada preferencia al votar, sin más que telefonear a ese número. Más evidente aún es el caso en que el remitente del mensaje incluye en el mismo datos identificativos adicionales con la intención de participar en un «*casting*».

Este criterio ha sido recientemente ratificado por la Audiencia Nacional en Sentencia de 8 de marzo de 2002 (procedimiento ordinario 948/2000). Según se cita en la misma, «*para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados*» y añade, que «*para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona*». La Sentencia se fundamenta precisamente en el contenido del artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, que considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Otra consideración adicional se refiere al responsable del tratamiento de datos, de cuya identidad y dirección (o bien de la de su representante) es preciso informar en el momento de la recogida de datos. Como ya se ha mencionado, las compañías que prestan los servicios de audiotex en acciones comerciales que llevan asociado un sorteo suelen ser contratadas por las cadenas de televisión. Sin embargo, no siempre le queda claro al participante a quién corresponde la responsabilidad del fichero al que se incorporarán sus datos personales, dado que las locuciones utilizadas no informan adecuadamente a este respecto. De forma análoga sucede cuando dichos servicios se aplican a procesos de selección de concursantes, siendo contratados los servicios en tales casos por la productora del concurso. Lo que sí resulta evidente, a la vista de todo ello, es que cuando el ciudadano realiza su llamada telefónica se puede sentir indefenso al no tener conocimiento de los destinatarios concretos de los datos que facilita (la productora, la compañía de televisión o la propia compañía de audiotex), ni de la finalidad con la que podrían ser tratados al margen de la que justifica la llamada.

Cuando la recogida de datos se realiza a través de mensajes cortos SMS el participante no recibe en ningún caso la preceptiva información sobre protección de datos, la cual debería facilitarse en el mismo momento en que se promociona el servicio, es decir, cuando se da publicidad (en los medios de comunicación) al número telefónico de cuatro cifras al que se remitirán los mensajes. Esto es aplicable tanto en los sorteos (asociados generalmente a líneas de votación) como en los procesos de selección de concursantes, donde los datos personales son más completos. Es quizás en estos servicios donde la desinformación tenga mayor trascendencia, pues, en este caso, se difumina la responsabilidad de las productoras o de las televisiones al ser las compañías que los prestan las que tienen la capacidad de conservar los mensajes en sus equipos por tiempo indefinido, no existiendo en los contratos, sin embargo, ningún reconocimiento de responsabilidad al respecto de los datos por parte de ninguna de las entidades implicadas.

Algo parecido ocurre cuando se solicita que los datos se envíen por vía postal, pues no se utilizan formularios al efecto, lo que, bien es verdad, ocurre cada vez en menos ocasiones, quizás debido a los importantes beneficios económicos que pueden reportar las otras vías de participación del público.

Cuando la recogida de datos se realiza a través de Internet se ha verificado que tampoco siempre se suministra la mencionada información, a pesar de que esta vía es la que más posibilidades ofrece y la que resulta menos onerosa para el ciudadano. En este sentido, es preciso recordar que el apartado 2 del citado artículo 5 de la LOPD establece que «*cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior*».

Por otra parte, son escasas las ocasiones en las que se informa (a través de las locuciones telefónicas, publicidad o Internet) de la posibilidad que tienen los participantes en estos eventos de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Calidad de los datos

Tal y como establece el 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*». A este respecto, aun cuando parece justificada la recogida de datos identificativos en los procesos de selección, no resulta tan defendible que el interesado deba facilitar gran cantidad de estos datos (que a veces incluyen, aparte del nombre y apellidos, el número de D.N.I. o la profesión) cuando la finalidad inicial de una línea de votación es que la audiencia pueda manifestar una cierta preferencia. Así resulta llamativo que, aunque en estos casos se ofrezca como compensación la participación en un sorteo, sean diferentes los datos que se recaban a través de un número 906 de los que se obtienen vía SMS, para una misma línea de votación. En este sentido, parece obvio que si en esta última vía de participación basta un número telefónico de contacto (que coincide con el que corresponde al terminal desde el que se envía el mensaje) para localizar al ganador del sorteo, también sería suficiente este dato para localizarlo entre los participantes que han llamado al número 906. No se entiende así que sean precisos otros datos para la finalidad perseguida, aunque es evidente que su solicitud tiene como consecuencia una mayor duración de la llamada y así un mayor importe en la factura telefónica del participante y, consiguientemente, un mayor ingreso económico para la compañía de audiotex y para la compañía contratante del servicio.

Al respecto de la pertinencia en la recogida de los datos cabe mencionar nuevamente los casos, ya comentados, en los que esta actividad resulta generadora de ingresos a los contratantes del servicio audiotex, pero no está justificada desde la perspectiva de protección de datos personales, al obtenerse tales datos sin que vayan a ser en absoluto utilizados para la finalidad supuestamente prevista.

Por otra parte, el apartado 2 del mismo artículo de la LOPD prevé 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*». A este respecto, no se ha detectado ningún caso en el que los datos recabados a través de un 906 o de SMS se hubiesen utilizado para otra finalidad que la que ocasionó su recogida. No obstante, sí se ha observado que alguna cadena de televisión había previsto añadir a los ingresos económicos que supone el servicio de valor añadido los que podrían resultar de la utilización comercial de los datos personales recabados. Así en los contratos firmados con la compañía de audiotex, relativos a los procesos de votación para medir el índice de popularidad de los concursantes de uno de los programas que más proyección pública han alcanzado, se prevé que «*los datos personales de los llamantes podrán ser utilizados para los fines comerciales que* [la cadena de TV y la compañía de audiotex] *estimen oportunos, siempre cumpliendo con la legislación vigente de protección de datos informatizados*». A pesar de ello y de que en las correspondientes

locuciones telefónicas ni siquiera se informaba a los participantes de la incorporación de sus datos a un fichero, no se ha obtenido constancia de que tales datos se hayan utilizado hasta la fecha con otros fines comerciales ni por la televisión ni por la compañía de audiotex.

En otro orden de cosas, el apartado 5 del artículo 4 de la LOPD 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» y que «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»*. En este sentido, se ha verificado que, generalmente, una vez que se han celebrado los sorteos, las compañías de audiotex borran de sus servidores los ficheros que contienen las grabaciones de voz con los datos de los participantes, concurriendo una motivación puramente práctica: el gran volumen de espacio en disco que suelen ocupar este tipo de ficheros. Se ha comprobado que, en algunos casos, se han establecido procedimientos para evitar la conservación de tales ficheros más de quince días desde la celebración del sorteo, pero en general puede decirse que no existen normas estrictas al respecto.

Por otra parte, en el caso de los mensajes SMS se ha constatado que no se han implantado aún procedimientos efectivos para el borrado periódico de los mismos, una vez concluidas las actividades que los originan. Así, la Inspección ha verificado que, por ejemplo, cierta compañía especializada en estos servicios conserva en sus servidores prácticamente la totalidad de los mensajes recibidos desde el comienzo de su actividad, lo que le aporta gran cantidad de información acerca del comportamiento de cada uno de los usuarios del servicio (identificados por su número de teléfono móvil), en relación con este tipo de eventos. No obstante, no se ha obtenido constancia de que esta información haya sido tratada hasta el momento con otros fines.

Respecto de las fichas manuales que elaboran las productoras durante los procesos de selección de concursantes, se ha observado que en ciertos casos son conservadas por estas compañías para ser utilizadas, en algunos casos, en sucesivos procesos de «*casting*», al considerar que en determinados programas los interesados responden a una misma tipología, en lo relativo a sus aptitudes artísticas, aficiones y valores personales.

Datos especialmente protegidos

No se ha obtenido evidencia de que en los programas de televisión analizados en el presente plan se traten datos de los que el artículo 7 de la LOPD considera especialmente protegidos: ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual. No obstante, la Agencia tiene constancia por actuaciones previas de que en el «*casting*» de determinados concursos se recaba información acerca de la vida sexual de los aspirantes, al ser éste un condicionante de la forma en que se plantearán sus relaciones de conviven-

cia durante el desarrollo del programa. Al respecto de esa información cabe distinguir entre las propias declaraciones de los aspirantes y las impresiones o percepciones de los entrevistadores durante el proceso de selección, que pueden, por ejemplo, referirse a la orientación sexual de los candidatos. En ambos casos, sin embargo, se requiere que el afectado lo consienta expresamente, de acuerdo con lo previsto en el artículo 7.3 de la LOPD. Así, debe tenerse en cuenta que tales datos no podrán ser recabados ni tratados durante el proceso de selección cuando no medie este consentimiento expreso del aspirante.

En este mismo tipo de concursos, por otra parte, participan en ocasiones profesionales especializados que obtienen perfiles de personalidad y valoraciones psicopatológicas de los aspirantes, a través de tests específicos, los cuales, en ciertos casos, podrían constituir evaluaciones acerca de la salud mental, por lo que deberían también atenderse las garantías legalmente previstas en el citado artículo 7.3, es decir, que se obtenga previamente el consentimiento expreso de los afectados.

Acceso a los datos por cuenta de terceros

Como ya se ha comentado, también en el negocio televisivo son numerosos los agentes implicados, aparte de las productoras y televisiones, que generalmente pueden ser considerado responsables de los correspondientes tratamientos y ficheros. Ello se justifica por la necesidad de que en ocasiones acceda a los mismos un tercero, para la prestación de un servicio al responsable, ya sea éste la atención de llamadas telefónicas, la recepción de mensajes de telefonía móvil, la transcripción informática de llamadas, la gestión de bases de datos, el alojamiento de páginas web o el mantenimiento del equipamiento informático. Pues bien, se ha comprobado que no siempre la realización de tratamientos por cuenta de terceros está regulada contractualmente en los términos previstos por el artículo 12 de la LOPD, lo que llevaría a considerar que tales accesos son en realidad comunicaciones de datos, siéndoles de aplicación el régimen establecido en el artículo 11.

En general, la productora de un formato televisivo y la cadena de televisión que lo emite están vinculadas contractualmente, aunque no se regula documentalmente el tratamiento que ambas realizan respecto de los datos personales de la audiencia. Tal como ya se ha comentado, ambas compañías suscriben a su vez contratos bilaterales con las compañías de audiotex o de recepción de mensajes SMS, que actúan *como «encargado del tratamiento»*, respecto de ficheros cuya responsabilidad podría corresponder a la productora (en el caso de los procesos de selección de concursantes) o a la compañía de televisión (en los sorteos asociados a líneas de votación o similares). Estos contratos, sin embargo, cuando existen documentalmente, no siempre especifican quién es el responsable del fichero y en ocasiones sólo hacen una vaga referencia al carácter confidencial de la prestación del servicio, no detallando las condiciones en que debería realizarse éste. En este sentido, no siempre se establece 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», tal como prevé el apartado 2 del citado artículo 12. De la misma manera, tampoco siempre se estipulan contractualmente las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Esta ausencia de normas documentadas es comparablemente más frecuente en los servicios automáticos (906 o SMS) de recogida de datos que se prestan para la celebración de sorteos, aunque son éstos más numerosos que los que se prestan en los procesos de selección de concursantes. Es especialmente notable, así mismo, que tampoco en tales casos se estipule el destino de los datos una vez cumplida la prestación contractual, a pesar de lo que establece el apartado 3 del artículo 12 de la LOPD. Como ya se ha comentado, los datos recogidos a través de los 906 no se conservan generalmente durante un largo período después del sorteo, aunque no ocurre lo mismo con los que se obtienen a través de mensajes SMS.

Ya se ha mencionado que una práctica muy común en el sector de audiotex es la compartición del tráfico de llamadas en situaciones de congestión de la red telefónica. Esta situación tiene graves consecuencias pues ocasiona que, a veces, los interesados puedan creer que están facilitando sus datos a una compañía de televisión cuando en realidad los están recibiendo, a través de sus propios servidores, compañías que no están vinculadas contractualmente con ésta. Es más, según se ha podido comprobar, las compañías que reciben las llamadas desviadas y, por tanto, los datos personales de los participantes, ni siquiera han suscrito contrato con la compañía a la que se encarga el servicio de audiotex. El resultado es que no existen garantías para los interesados respecto del tratamiento que se dará a los datos facilitados telefónicamente.

Comunicación de datos

En este apartado cabe insistir nuevamente en los casos en que la finalidad inicial de los datos recogidos, la participación en un sorteo o en un concurso, se desvía para su tratamiento en actividades comerciales, de publicidad o marketing, las cuales son generalmente realizadas por otras compañías, lo que constituye una comunicación de datos. Es preciso recordar lo que establece el 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*».

De este precepto se desprende que tal comunicación sólo podría realizarse cuando el participante en el sorteo o concurso tenga conocimiento de la misma y la haya consentido previamente, lo que no ocurre en los casos analizados, pues, como ya se ha repetido en varias ocasiones, la información suministrada en la recogida, cuando se facilita, es más bien escasa.

A este respecto, se ha tenido conocimiento de que una cadena de televisión comercializó en el pasado datos personales de concursantes, al ofrecérselos a una compañía que los recopilaba con fines de marketing directo para alquilarlos a las empresas interesadas, actividad esta que suele conocerse como »*listbroking*». Así, en el contrato correspondiente la cadena de TV exponía que «*como consecuencia del normal ejercicio de las actividades que conforman su objeto social, ha devenido poseedora de un cúmulo de datos de personas y empresas que, por motivos varios, han tenido algún tipo de trato con la entidad».* La compañía de marketing, por su parte, se reconocía «*consciente de las oportunidades comerciales que dicho banco de datos es susceptible de generar*» y se comprometía a actuar como agente para la explotación comercial del fichero. Según ha declarado la responsable del fichero, la única iniciativa que se llevó a cabo en materia de protección de datos, antes de alquilar el fichero, fue cruzarlo con la Lista Robinson de la Asociación Española de Marketing Directo, acción ésta que no aseguraría el cumplimiento de la legislación vigente pues no garantiza el consentimiento de los interesados para la utilización comercial de sus datos. No obstante, el tiempo transcurrido hace que esta conducta, que podría ser constitutiva de infracción, haya superado ya los plazos de prescripción legalmente previstos.

Se da la circunstancia de que precisamente la Agencia ha iniciado hace unos meses un Procedimiento Sancionador a la citada compañía de marketing, como consecuencia de una denuncia presentada por un concursante de un programa emitido por la misma cadena de televisión, al haberse obtenido evidencias de que la productora del programa le había vendido a aquélla las cartas recibidas con datos de personas interesadas en concursar en otro programa.

Movimiento internacional de datos

En general, se puede decir que en el sector de actividad analizado no son frecuentes las transferencias de datos de carácter personal a otros países, dado que tanto las productoras como las televisiones suelen ser sociedades establecidas en nuestro país.

Sin embargo, al igual que en otras actividades comerciales, siguen existiendo compañías que optan por encargar los servicios informáticos, especialmente el alojamiento de páginas web cuando éste lleva asociada la recogida de datos personales en Internet, a otras entidades especializadas que, en ocasiones, se han establecido en países que no son miembros de la Unión Europea, o respecto de los cuales la Comisión de las Comunidades Europeas no haya declarado que garantizan un nivel de protección adecuado.

Es significativo que uno de los países más frecuentemente elegidos siga siendo precisamente Estados Unidos de América. A este respecto, la Comisión Europea ha adoptado una Decisión, publicada en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000, considerando la existencia de un nivel de protección adecuado cuando las empresas destinatarias de los datos se adhieran a los principios del puerto seguro y a las correspon-

dientes preguntas más frecuentes publicadas por el Departamento de Comercio Norteamericano. En otro caso, la compañía está obligada a solicitar la correspondiente autorización del Director de la Agencia, conforme a lo dispuesto en el artículo 33 de la LOPD, a menos que concurra alguna de las excepciones previstas en el artículo 34. En este sentido, el responsable del fichero puede optar, por ejemplo, por acogerse a la excepción prevista en el apartado e) del citado artículo 34: «*que el afectado haya dado su consentimiento inequívoco a la transferencia prevista*», para lo cual deberá informar adecuadamente en los formularios utilizados en la recogida de datos.

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

Como continuación a lo ya expuesto en el apartado 3.1, es preciso señalar que la consecuencia inmediata de la falta de una información clara en la recogida de datos personales es, precisamente, que se puedan ver vulnerados los derechos de los ciudadanos, pues éstos no saben con exactitud cuál es la entidad que se hace responsable del fichero al que se incorporan sus datos, ni el domicilio al que pueden dirigirse para ejercer sus derechos de acceso, rectificación, oposición y cancelación. No obstante, durante el desarrollo de las presentes actuaciones se ha podido comprobar que gran parte de las entidades implicadas han modificado el contenido de las locuciones telefónicas para incorporar esta información.

Seguridad de los datos

De conformidad con lo que establece el Reglamento de Medidas de Seguridad, aprobado mediante Real Decreto 994/1999, de 11 de junio, se ha comprobado que, en general, las televisiones han elaborado e implantado su propia normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y al conjunto de los sistemas de información corporativos.

No puede decirse lo mismo, sin embargo, de las productoras y de las compañías que prestan servicios de audiotex o de recepción de mensajes SMS. En general se trata de compañías que se hallan en un proceso de implantación de las medidas de seguridad, por lo que los documentos de referencia, cuando existen, suelen tener carácter provisional. En este sentido, hay que recordar que, tanto si la compañía actúa como responsable del fichero como si lo hace en calidad de encargado del tratamiento, el artículo 9 de la LOPD establece que deberán adoptarse *«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».*

Por otra parte, se ha observado que es frecuente el intercambio a través de Internet de ficheros con datos personales entre las distintas compañías que participan en la realización de programas de televisión. Aunque puede decirse que la mayor parte de los ficheros analizados presentan una estructura de datos tal que, en aplicación del artículo 4 del Regla-

mento, cabría exigir la adopción de las medidas de seguridad calificadas como de nivel básico, es preciso incidir en los riesgos asociados al envío de tales datos a través de un medio que ofrece tan pocas garantías de seguridad como es Internet. A este respecto hay que mencionar la sanción impuesta por la Agencia en el año 2000 a la productora de un concurso, al no haber estipulado contractualmente las medidas que debían adoptar todas las entidades colaboradoras con objeto de evitar que los datos recabados durante el proceso de selección de participantes llegasen a hacerse públicos a través de la Red, como finalmente ocurrió. También hay que recordar que, tal y como establece el artículo 23 del Reglamento para los ficheros sobre los que son exigibles medidas de nivel alto, *«la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte».*

Notificación e inscripción registral de los ficheros

Se ha observado que durante el desarrollo de las presentes actuaciones han sido numerosas las compañías del sector que han notificado nuevos ficheros a la Agencia para su inscripción en el Registro General de Protección de Datos, siendo la mayor parte de ellas las que realizan las labores de producción, haciendo constar en algunos casos que el tratamiento de datos ha sido encargado a compañías especializadas en audiotex.

También es destacable que no son numerosos los ficheros inscritos en relación con la recepción de mensajes SMS, quizás porque no existe conciencia de que el almacenamiento de tales mensajes, junto con el número del remitente, constituye en sí mismo un tratamiento de datos personales, de acuerdo con la argumentación ya desarrollada en este documento.

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, dicta las siguientes recomendaciones, que deberán ser observadas por todas las compañías implicadas en la producción y realización de programas de televisión, al objeto de adecuar éstas a los principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y a la normativa que la desarrolla.

Primera: Información en la recogida de datos

1. De conformidad con lo establecido por el 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.

2. Esta información deberá ser facilitada con carácter previo independientemente de la vía a través de la cual se recaben datos personales, ya sea a través de líneas telefónicas, mensajes SMS, correo postal, Internet o cualquier otra. Cuando el medio utilizado no permita el contacto simultáneo con el interesado en el momento en el que éste facilita sus datos, el responsable se asegurará de que se le suministra la citada información en el momento en que se da publicidad al procedimiento por el que se recibirán los datos.

3. La citada información se facilitará cualquiera que sea la tecnología utilizada para el almacenamiento de los datos, ya se trate de ficheros de audio o ficheros convencionales de texto en formato ASCII o cualquier otro.

4. Esta misma información se suministrará independientemente de la tipología de datos personales que se recaban, entendiéndose a estos efectos que, en el contexto que nos ocupa, el número de teléfono (fijo o móvil) es por sí mismo un dato personal de carácter identificativo y que, por tanto, la información asociada al mismo puede concernir a una persona física identificable.

5. De acuerdo con lo que establece el apartado 2 del artículo 5 de la LOPD, esa misma información debe figurar en forma claramente legible cuando se utilicen cuestionarios u otros impresos para la recogida, por lo que en tales casos no basta la comunicación verbal de tales advertencias.

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

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. A este respecto, se entenderá que cuando el afectado facilita voluntariamente sus datos consiente en el tratamiento de los mismos en los términos y condiciones de los que ha sido convenientemente informado en el momento de la recogida.

Tercera: Usos y finalidades

1. 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.

2. No se recabarán 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. En particular, no se recabarán datos personales a través de líneas 906 cuando éstos no vayan a ser utilizados para la finalidad comunicada y su recogida sólo éste motivada por cuestiones promocionales.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. A este respecto debe recordarse que la Sentencia 292/2000 del Tribunal Constitucional ha señalado que «*el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros [...] Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado*». Así, para que tales datos puedan ser usados para una finalidad distinta, es imprescindible obtener previamente el consentimiento inequívoco del afectado.

Cuarta: Cancelación de datos

1. 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.

2. Esta obligación se extiende a cualquiera de los ficheros o tratamientos especificados en la Recomendación Primera, siempre y cuando los datos de carácter personal no deban 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.

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.

Sexta: Acceso a los datos por cuenta de terceros

1. 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.

2. 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.

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

4. Estas obligaciones se extenderán a todas aquellas entidades que, como encargados del tratamiento, participen en la realización de los programas de televisión. 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.

5. En particular, la colaboración de distintas entidades en la atención de líneas telefónicas en situaciones de congestión de red deberá regularse en todo caso de acuerdo con lo expresado en los apartados anteriores.

Séptima: Comunicación de datos

1. 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 desa-

rrollo, 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.

2. 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 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.

Octava: Movimiento internacional de datos

1. 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.

   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 datos personales (recabados a través de Internet o por cualquier otra vía) 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.

2. De acuerdo con lo que establece el artículo 5 de la LOPD, 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.

3. 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.

4. 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.

Novena: Seguridad de los datos

1. 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.

2. 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.

3. Se considera una buena práctica la adopción de medidas que eviten que la información circule por Internet de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros.

2.2.2. *Censos de Población y Vivienda 2001*

Por acuerdo del Director de la Agencia de Protección de Datos se procedió por parte de la Inspección de Datos a realizar un Plan de Inspección de Oficio al Proyecto *Censos de Población y Viviendas 2001*.

Las actuaciones de investigación en los *Censos de Población y Viviendas 2001* se han desarrollado durante un periodo que abarca los años 2001 y 2002. Por ello, en la Memoria del ejercicio de 2001 ya se informó acerca de los objetivos del plan, de la legislación aplicable en el ámbito del Proyecto y de las actuaciones practicadas por parte de la Inspección de Datos en dicho periodo. Del resultado de las investigaciones efectuadas se detectaron cier-

tas deficiencias en relación con las contrataciones efectuadas por el Instituto Nacional de Estadística (I.N.E.), que implicaban un acceso por cuenta de terceros a los Sistemas de Información cuya titularidad corresponde al citado Instituto y cuya subsanación supondría una sustancial mejora en el acatamiento de la Ley Orgánica 15/1999.

A tal efecto, el Director de la Agencia de Protección de Datos dictó las correspondientes Recomendaciones al I.N.E. al objeto de adecuar plenamente los tratamientos automatizados a los principios de la citada Ley y de la normativa que la desarrolla. Dichas Recomendaciones se describieron en la Memoria del ejercicio 2001.

Las actuaciones desarrolladas por parte de la Inspección de Datos en el ámbito del proyecto se han referido tanto al I.N.E. como a las empresas participantes en el mismo.

En relación a estas últimas debe destacarse las investigaciones relacionadas con la prestación de servicios informáticos para la operación, gestión y control de un sistema orientado a la captura y depuración de la documentación censal y para el desarrollo e implementación de un sistema de gestión y reconocimiento automático de la misma; así como para la distribución, recogida y destrucción de la documentación utilizada.

La participación de entidades de distinta naturaleza, como son las señaladas, aconsejó que, una vez finalizados los trabajos de inspección, se formularan por separado las respectivas conclusiones y recomendaciones.

Las primeras se transcriben a continuación bajo rúbricas diferenciadas. De las segundas, al haberse adoptado en el año 2003, se dará cuenta en la memoria correspondiente a dicho ejercicio.

Conclusiones al Instituto Nacional de Estadística

Del análisis de las actuaciones efectuadas por parte de la Inspección de Datos en el ámbito de los *Censos de Población y Viviendas 2001*, desde el punto de vista de la adecuación legal a los principios de la Ley Orgánica de Protección de Datos de Carácter Personal y de la Ley de la Función Estadística Pública, se derivan las siguientes conclusiones.

Tratamientos preliminares

El Reglamento de Población y Demarcación Territorial de las Entidades Locales establece el nuevo marco de relación entre *Censo de Población* y *Padrón Municipal de Habitantes.* En este sentido dispone que *«La formación del censo de población, que constituye una competencia exclusiva del I.N.E., se apoyará en los datos de los padrones municipales y servirá para controlar la precisión de los datos padronales y, en su caso, para introducir en ellos las rectificaciones pertinentes».*

Con la finalidad de mantener debidamente actualizados los datos que con carácter obligatorio deben de figurar en el padrón municipal, los distintos organismos de la Administración General del Estado deben remitir periódicamente a cada Ayuntamiento los datos que afectan a sus vecinos. Entre dichos organismos se encuentran las Oficinas del Registro Civil en lo relativo a nacimientos, defunciones, cambios de nombre, de apellidos, de sexo y de nacionalidad y el Ministerio del Interior en cuanto a expediciones de documentos nacionales de identidad y de tarjetas de residencia. Las citadas comunicaciones de datos pueden ser canalizadas a través del I.N.E., ya que dicho Instituto podrá llevar a cabo el control de la precisión de los Padrones y proponer a los Ayuntamientos la realización de operaciones conjuntas, según prevé dicho Reglamento.

De conformidad con lo anteriormente expuesto, el I.N.E. procedió a la validación de la información suministrada por los Ayuntamientos, por el Ministerio del Interior, por el Registro Civil y por la Dirección General del Catastro con objeto de facilitar a los ciudadanos la cumplimentación de los censos. Por ello, en la *Hoja Padronal*, que fue facilitada a los ciudadanos conjuntamente con los *cuestionarios censales*, se encontraba impresa la información de que disponían las Administraciones Públicas en relación con los datos padronales.

Contenido de los Cuestionarios Censales

El I.N.E. utilizó como instrumentos para la recogida de información en los *Censos de Población y Viviendas 2001* los documentos denominados *cuestionarios censales*, cuyos modelos básicos se publicaron en el anexo II de la Orden de 23 de abril de 2001, del Ministerio de la Presidencia, por la que se dictan instrucciones para la formación de dichos censos.

Con anterioridad a la publicación de la citada Orden, el contenido y formato de los cuestionarios *vivienda, hogar e individual* y *Hoja Padronal*, fueron informados por parte del Director de la Agencia de Protección de Datos en los términos siguientes: «*dicho cuestionario cumple con el principio de proporcionalidad, esencial para el cumplimiento de lo Previsto en la Ley 12/1989, dado que existe una adecuada correlación entre la información solicitada y el resultado que de la misma se pretende obtener*».

En cuanto al contenido de la *Hoja Padronal*, la Ley Reguladora de las Bases del Régimen Local dispone que el Padrón Municipal contendrá como obligatorios los siguientes datos: «*nombre y apellidos, sexo, domicilio habitual, nacionalidad, lugar y fecha de nacimiento, número de documento nacional de identidad o documento que lo sustituya, certificado o título escolar o académico que se posea y cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales recogidos en la Constitución*». Dichos datos coinciden con los que se solicitaban mediante la *Hoja Padronal* que, inicialmente, se encontraban impresos con la informa-

ción de que disponía el I.N.E., por lo que el ciudadano debía comprobar su exactitud y, en su caso, realizar las modificaciones oportunas.

De las actuaciones efectuadas por parte de la Inspección de Datos se verificó que la tipología de la información censal recabada por medio de los cuestionarios se corresponde con la que fue informada por parte del Director de la Agencia de Protección de Datos, con la que establece la Ley Reguladora de las Bases del Régimen Local y con la que fue aprobada mediante Orden Ministerial de 23 de abril de 2001. Por otra parte, se constató que el contenido de los cuestionarios que el ciudadano podía cumplimentar a través de Internet coincidía con el de los cuestionarios en papel.

Calidad de los datos

Entre los principios de la protección de datos se encuentra el de *calidad*, artículo 4 de la Ley Orgánica, que establece que «*los datos de carácter personal sólo se podrán recoger para su tratamiento, cuando sean adecuados pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas*» y que «*no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos*». Dicho principio se encuentra íntimamente ligado a los principios de especialidad y proporcionalidad recogidos en el artículo 4 de la Ley de la Función Estadística Pública, cuyos conceptos se transcriben a continuación:

- Especialidad: «*es exigible a los servicios estadísticos que los datos recogidos para la elaboración de estadísticas se destinen a los fines que justificaron la obtención de los mismos*».

- Proporcionalidad: «*se observará el criterio de correspondencia entre la cuantía de la información que se solicita y los resultados que de su tratamiento se pretende obtener*».

De acuerdo con ello, se establecieron documentos distintos para recabar la información padronal y censal con objeto de preservar la naturaleza de ambos. Aunque la finalidad del *Censo de Población* y la del *Padrón Municipal* siempre ha sido distinta, por una parte estadística y por otra administrativa, la formación conjunta de ambos documentos ha permitido que las cifras que se han deducido de los mismos sean coincidentes.

Conservación de la información y documentación censal

La información recabada en la *Hoja Padronal*, una vez validada por el I.N.E., fue remitida a los Ayuntamientos con objeto de revisar el Padrón Municipal y mantener actualizados los datos padronales por ambas instituciones, según prevé el Real Decreto 2612/1996, sobre gestión, control y revisión del padrón municipal.

Por otra parte, la imagen digitalizada de la *Hoja Padronal* se facilitó a los Ayuntamientos como acreditación de las propuestas de variación o aceptación de los datos padronales por parte del ciudadano. En este sentido, debe señalarse que los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación, en virtud de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. A tal efecto, el propio I.N.E. conserva la imagen digitalizada de la *Hoja Padronal* y la documentación en soporte papel ha sido destruida.

En relación con la información censal recabada en los cuestionarios *vivienda, hogar e individual,* debe señalarse que la base de datos censal anonimizada resultado de los procesos de captura y validación de la información incluida en los cuestionarios, en la que los datos han sido sometidos a los procesos inherentes al tratamiento estadístico de la información, será conservada y custodiada de forma permanente por el I.N.E.

Los *cuestionarios censales* han sido tratados por el I.N.E. en el ejercicio de sus funciones, dado que carecen de valor probatorio, puesto que la información recabada sólo puede utilizarse con fines estadísticos, el soporte papel ha sido destruido, con autorización de la Administración competente, mediante el procedimiento reglamentariamente establecido, y los ficheros que contienen la imagen digitalizada de los mismos también pueden ser borrados.

Información facilitada en la recogida de datos

En cuanto a la información facilitada a los ciudadanos por parte del I.N.E. en los procedimientos de recogida de datos es preciso señalar lo siguiente:

- Respecto a los cuestionarios en papel:

  En el reverso del *cuestionario vivienda* figuraban aspectos relativos al «*secreto estadístico*», «*obligación de facilitar los datos*» *y «las sanciones por no colaborar».* Conjuntamente con el sobre que contenía los *cuestionarios censales* se distribuyó en las viviendas un tríptico en el que se informaba de «*La utilidad de los Censos*», del *«Secreto Estadístico»* y de que *«las modificaciones que realice en los datos padronales serán trasladadas por el I.N.E. a los Ayuntamientos para su repercusión en el Padrón Municipal».*

  En cuanto al derecho de información que establece el artículo 5 de la Ley Orgánica 15/1999, en el citado tríptico figuraba un apartado relativo a «*protección de datos*» en el que constaba que, «*Los datos que facilite en la cumplimentación de los cuestionarios quedan amparados por el secreto estadístico y no se podrán utilizar con ninguna*

finalidad distinta de la producción estadística. Sólo las posibles modificaciones a sus datos padronales, serán remitidas a su Ayuntamiento, que es el responsable de la gestión del Padrón de Habitantes, y ante el que puede ejercer, si lo desea, los derechos de acceso y rectificación de los datos padronales, previstos en la Ley Orgánica de Protección de Datos de Carácter Personal».

- Respecto a la cumplimentación vía Internet:

  Aunque en un principio se tenía previsto presentar un texto «*informando sobre la política de confidencialidad de la información seguida para la protección de los datos*», finalmente dicho texto no fue incluido.

  Sin embargo, se podía acceder a una página específica en la que figuraba: «*La información que nos facilite está amparada por el secreto estadístico; por tanto, no será publicada ni cedida a nadie de manera que se pueda saber a quién corresponde, ni siquiera indirectamente. La única excepción son las posibles modificaciones que necesiten sus datos padronales, que el INE debe enviar, para que se actualice el Padrón de Habitantes, a su Ayuntamiento, ante el que puede ejercer, si lo desea, los derechos de acceso y rectificación previstos en la Ley Orgánica de Protección de Datos de Carácter Personal».* Por lo que no figuraba información de la obligación o no de facilitar los datos y de las consecuencias de su no colaboración o de suministrar datos falsos.

- Respecto a la información recabada en el Centro de Atención a Usuarios:

  En el Centro de Atención a Usuarios, dónde se atendían las consultas efectuadas por los ciudadanos en relación con la cumplimentación de los censos, hay que distinguir entre los datos personales que se obtienen telefónicamente y los que se recaban a través del correo electrónico. En general, se requería de los ciudadanos los datos relativos al sexo, edad, provincia e idioma con objeto de realizar estadísticas de las actividades efectuadas en el Centro. Sólo en el caso de que la llamada telefónica hubiera requerido la intervención directa del I.N.E. se solicitaban los siguientes datos adicionales: nombre, apellidos, teléfono, fecha y hora, junto a la descripción de la correspondiente reclamación. Todos estos datos eran enviados al I.N.E. a través de correo electrónico y, en ningún caso, se informaba al interesado de lo que establece el artículo 5 de la precitada Ley Orgánica.

  Por otra parte, los interesados disponían de otra vía para dirigirse al I.N.E.: el correo electrónico, facilitando el remitente voluntariamente el nombre, apellidos y dirección electrónica. Respecto del tratamiento de estos datos, no se incluía en el sitio web ninguna otra información aparte de la que se ha referido anteriormente relativa al secreto estadístico.

Consentimiento del afectado

El I.N.E. no ha solicitado el consentimiento de los ciudadanos para el tratamiento automatizado de los datos de carácter personal facilitados en los *cuestionarios censales* y en la *Hoja Padronal*. No obstante, sobre este aspecto se debe tener en consideración que:

- El apartado octavo de la Orden del 23 de abril de 2001, del Ministerio de la Presidencia, establece que «*Las personas físicas y jurídicas estarán obligadas a aportar los datos censales que se solicite en aplicación de la Ley de la Función Estadística Pública. La no cumplimentación de los cuestionarios o el suministro de datos incompletos o falsos podría ser sancionada conforme se establece en los artículos 50 y 51 de la mencionada Ley 12/1989*».

- La disposición adicional cuarta de la Ley 4/1990, de Presupuestos Generales del Estado establece «*De conformidad con lo establecido en el artículo 7 de la Ley 12/1989, de la Función Estadística Pública, se consideran estadísticas de cumplimentación obligatoria las siguientes: a) Censos de población y viviendas. b) Censos de edificios y locales. c) (...)*».

- Mediante Real Decreto 1126/2000, de 16 de junio, se Aprueba el Plan Estadístico Nacional 2001-2004, en virtud del artículo 2 «*Tienen la consideración de estadísticas para fines estatales todas las incluidas en el Plan Estadístico Nacional y son de cumplimentación obligatoria*». En el anexo I de dicha norma figura la relación de las estadísticas que han de elaborarse en el cuatrienio figurando en el tema «*Demografía y Población*» la operación estadística denominada «*Censos de Población y Viviendas*».

A este respecto, hay que señalar que el artículo 6 de la Ley Orgánica 15/1999 prevé que, «*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de la Administraciones Públicas en el ámbito de sus competencias*».

Por ello, en virtud de las prescripciones legales transcritas los datos de carácter personal recabados por el I.N.E. se enmarcan en el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Así mismo, no se ha constatado que el I.N.E. proceda a recabar y automatizar datos personales que no estén autorizados por la normativa vigente y que no sean necesarios para el desempeño de las funciones que tiene encomendadas.

Datos especialmente protegidos

En los *cuestionarios censales* y en la *Hoja Padronal* utilizados por el I.N.E. para recabar la información relativa a los *Censos de Población y Viviendas 2001* no figuraban preguntas

que, directamente, hicieran referencia a datos especialmente protegidos en los términos que especifica la Ley Orgánica 15/1999 y la Ley 12/1989, como son: ideología, religión, creencias, origen racial, salud o vida sexual.
Sin embargo, analizando las preguntas que contenían los cuestionarios se plantean las cuestiones que, a continuación, se describen:

- *Sexo:* que figuraba en la *Hoja Padronal* y que es una información de carácter obligatoria para su incorporación al Padrón Municipal.

- *Relación de parentesco con la persona 1:* esta pregunta constaba en el *cuestionario hogar* y entre las posibles modalidades de respuesta se encontraba «*cónyuge o pareja, (...)*». La relación de parentesco combinada con el sexo, podría considerarse como información sobre las personas, tanto si son heterosexuales como homosexuales. Dicha información era necesaria para establecer la composición de las familias y los hogares, siendo una información útil para la formulación o seguimiento de políticas sociales y de investigaciones sociodemográficas. La persona enumerada en primer lugar correspondía, en general, con la primera persona que consta empadronada en la vivienda, ya que se encontraba impreso en este cuestionario el nombre de pila, la primera inicial de cada apellido y la fecha de nacimiento.

- *Estado civil:* pregunta que figuraba en el *cuestionario hogar.* Entre las modalidades de respuesta se encontraba «*soltero, casado, (...)*« correspondiendo a la situación legal de la persona. Esta información era necesaria para la evaluación de políticas sociales.

Por todo ello, combinando la información relativa al *estado civil*, *si tienes cónyuge o pareja* y *el sexo*, se podría extraer una estimación de las parejas de hecho y, en particular, de las homosexuales o heterosexuales. Ahora bien, la información relativa al *cónyuge o pareja* y al *estado civil*, se recaban en el cuestionario censal relativo al *hogar* siendo información con fines estadísticos, por lo que los citados tratamientos deben ser realizados sobre datos en los que se haya disociado la identificación de las personas a las que pertenecen.

Secreto Estadístico

En el ordenamiento jurídico vigente se exige de forma reiterada que el personal implicado en los trabajos censales tendrá la obligación de preservar el secreto estadístico, tanto el dependiente de los servicios estadísticos como el que participa con carácter eventual. Están también obligados por el deber de preservar el secreto estadístico las personas jurídicas con ocasión de su participación en virtud de contrato, acuerdo o convenio de cualquier género. Dicha obligación deberá mantenerse aún después de que las personas concluyan sus actividades profesionales o su vinculación a los servicios estadísticos.

A tal efecto el I.N.E. tomó las siguientes medidas:

- En los contratos suscritos por las personas que han participado en el Proyecto constaba una cláusula que indicaba que *«El trabajador queda obligado de conformidad con los art. 17.3 y 17.4 de la Ley de la Función Estadística Pública, a preservar el secreto estadístico, aún cuando después de que concluya su vinculación con el INE».*

- En los manuales que se entregaban a las personas que participaron en la *operación censal* figuraba el siguiente texto: «*los datos personales de los Censos quedan protegidos por el secreto estadístico. A quien viole el secreto estadístico se le podrán aplicar las sanciones previstas en los artículos 50 y 51 de la Ley de la Función Estadística Pública*». También, en la cinta de audio que se les entregaba se advertía sobre «*la confidencialidad de los datos que se van a recoger*». En el carnet acreditativo constaba que *«el portador de esta credencial está obligado a guardar secreto sobre la información que se le facilite según se indica en la Ley (...)».*

- En el Convenio suscrito con la Entidad Pública Correos y Telégrafos figuraba que *«el personal que participe en la recogida de la información se comprometerá a preservar el secreto estadístico en los términos establecidos en la Ley de la Función Estadística Pública».*

- Todas las personas físicas y jurídicas que participaron en el Proyecto para la prestación de servicios suscribieron, en los términos que establece el artículo 12 de la Ley Orgánica de Protección de Datos, el documento denominado «*Declaración de Empresa/Individual en Materia de Secreto Estadístico*» en el que declaraban «*Haber leído y comprendido*» el contenido de su reverso en el que figuran aspectos sobre «*El secreto estadístico*», «*Las obligaciones que impone*» y «*Las consecuencias de su vulneración*». Las empresas también se comprometían a que únicamente el personal que hubiera firmado dicho documento participara en el trabajo contratado, debiendo entregar al I.N.E. todas las declaraciones.

De otro lado, el Reglamento de Población establece en su artículo 79 que, *«la formación del Censo de Población, que constituye una competencia exclusiva del I.N.E., se apoyará en los datos de los Padrones municipales. En el desarrollo de esta operación se tomarán las medidas necesarias para mantener separados los datos censales, sometidos al secreto estadístico, de los padronales, de carácter nominal y con efectos esencialmente administrativos».*

A tal efecto, si bien el procedimiento de recogida fue único en ambos casos, los cuestionarios fueron diseñados mediante un sistema que permitía mantener separados los datos censales y los datos padronales.

Además, hay que tener en consideración que, para preservar la confidencialidad en el proceso de entrega de la documentación al ciudadano, en el caso de que no se pudiera facili-

tar en mano al destinatario, el *Agente Censal* podía dejarlos a terceras personas o en los buzones para lo cual debía introducirlos en un sobre sin ventanilla, cerrar el sobre y escribir el nombre y la dirección de las personas a las que la documentación iba dirigida. En cuanto a la recogida, el *Agente Censal* tenía la obligación de pasar por las viviendas para recabarlos. También se indicaba al ciudadano que los cuestionarios podrían ser devueltos a través del portero o algún vecino, dentro de un sobre sin ventanilla que tenía que facilitar el *Agente Censal* conjuntamente con el resto de la documentación. Dichos procedimientos se encontraban descritos en el capítulo tercero, «*material necesario: sobres sin ventanilla*», y en el capítulo quinto, «*entrega de cuestionarios*», del Manual del entrevistador que se entregó a los agentes censales.

Comunicación de datos padronales

Los datos padronales recabados en la *Hoja Padronal* o a través de Internet, en el ámbito de los *Censos de Población y Viviendas 2001*, fueron remitidos por parte del I.N.E. a los Ayuntamientos en soporte magnético. Dicho soporte contenía los ficheros automatizados con la información padronal y con la imagen digitalizada de dicho documento.

La citada comunicación de datos se realizó en virtud de lo previsto en el Reglamento de Población, que establece un intercambio de información padronal entre los Ayuntamientos y el I.N.E. y, en concreto, permite expresamente que dicho Instituto podrá «*llevar a cabo operaciones de control de la precisión de los Padrones municipales, informando del resultado a los correspondiente ayuntamientos, y comunicándoles, en su caso, las medidas a tomar para dotar a su Padrón de una mayor precisión».*

La imagen digitalizada de la *Hoja Padronal* se facilitó a los Ayuntamientos como acreditación de las propuestas de variación o aceptación de los datos padronales por parte del ciudadano, en virtud de lo previsto en la Ley 30/1992, antes citada.

Conjuntamente con el soporte magnético, la Presidenta del I.N.E. remitió a los Ayuntamientos un documento en el que informaba de diversos aspectos sobre la Ley Orgánica de Protección de Datos, como son que «*no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*», 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*», que »*quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal*» y que «*sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario».*

Por parte de la Inspección de Datos se constató que la información remitida a los Ayuntamientos en soporte informático, según el diseño de registro aprobado por Resolución de 20

de noviembre de 2001, del Ministerio de la Presidencia, no contenía los datos cifrados ni se había utilizado otro mecanismo que garantizara que dicha información no fuera inteligible, ni manipulada durante su transporte, al no ser exigida esta medida de seguridad en el Real Decreto 994/1999, atendiendo a la naturaleza de la información que contenían.

De las actuaciones efectuadas por parte de la Inspección de Datos no se ha podido constatar que el I.N.E., en el ámbito de los *Censos de Población y Viviendas 2001*, haya facilitado datos a terceros que no estuvieran autorizados en una Ley o en el ámbito de la prestación de un servicio contratado por dicho Organismo.

Comunicación de datos censales

El I.N.E. tiene previsto facilitar los datos personales recabados en los *Censos de Población y Viviendas 2001* a otras Administraciones Públicas cuando se cumplan los siguientes requisitos regulados en la Ley de la Función Estadística Pública:

- *«Que los servicios que reciban los datos desarrollen funciones fundamentalmente estadística y hayan sido regulados como tales antes de que los datos sean cedidos.*

- *Que el destino de los datos sea precisamente la elaboración de las estadísticas que dichos servicios tengan encomendadas.*

- *Que los servicios destinatarios de la información dispongan de los medios necesarios para preservar el secreto estadístico».*

Los datos que se han solicitado con ocasión de la *operación censal* serán usados exclusivamente con fines estadísticos. En particular, de las actuaciones efectuadas por la Inspección de Datos no se ha constatado que la información censal hubiera sido cedida a otros organismos.

Acceso a los datos por cuenta de terceros

El I.N.E. contrató la prestación de diversos servicios que implicaban tratamiento automatizado de datos de carácter personal a entidades privadas en el ámbito de los *Censos de Población y Viviendas 2001*, entre los que hay que mencionar los siguientes:

- *Personalización de los Cuestionarios Censales.*
- *Edición de los Cuadernos de Recorrido.*
- *Implementación y gestión de un Sistema Telemático para la cumplimentación vía Internet de los Censos de Población y Viviendas 2001.*
- *Implementación y gestión de un Centro de Atención al Usuario.*

- *Almacenamiento y distribución del material necesario para la realización de los Censos de Población y Viviendas 2001.*
- *Desarrollo e implementación de un Sistema de Gestión y Reconocimiento Automático (OCR) de la documentación censal.*
- *Servicios de carácter informático, para la operación, gestión y control de un sistema de producción orientado a captura y depuración de la documentación censal: recursos humanos.*
- *Destrucción de la documentación censal.*

La contratación de dichos servicios se realizó de conformidad con lo dispuesto en la Ley 13/1995, de 18 de mayo, de Contratos de las Administraciones Públicas y cumpliéndose las condiciones reguladas en el artículo 12 de la Ley Orgánica 15/1999.

También participaron diversos organismos públicos con los que se suscribieron los respectivos convenios o acuerdos de colaboración como el Instituto de Estadística de la Comunidad de Madrid, la Dirección General del Catastro y la Entidad Pública Empresarial Correos y Telégrafos.

Notificación a los ciudadanos de la información padronal

Los Ayuntamientos tienen la obligación de notificar, al menos una vez cada cinco años, los datos padronales a sus vecinos de manera que tengan la oportunidad de conocer la información que les concierne, en virtud de lo previsto en el artículo 69 del Reglamento de Población. En este sentido, los datos padronales que se imprimieron en la *Hoja Padronal* que se hizo llegar, junto con los *cuestionarios censales* propiamente dichos, a todas las personas que en ese momento estaban inscritas en el padrón sirvieron, legalmente, según acuerdo del Consejo de Empadronamiento para los fines establecidos en dicho Reglamento.

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

En relación con los datos padronales el I.N.E. informó, en los procedimientos de recogida, que el derecho de acceso y rectificación de los datos padronales previsto en la Ley Orgánica 15/1999, se debían ejercer ante el correspondiente Ayuntamiento. Por ello, cuando el ciudadano lo solicite se le deberá facilitar los datos de que dispone el Ayuntamiento incluidos en el fichero Padrón. Así mismo, podrá ejercer el derecho de rectificación aportando la documentación acreditativa. En el caso de que el ciudadano se empadrone en otro municipio, el propio I.N.E. procederá de oficio a las rectificaciones necesarias con objeto de que los datos de carácter personal sean exactos y respondan con veracidad a la situación actual del afectado, comunicando dicha modificación al Ayuntamiento afectado.

Con respecto a los datos censales, el I.N.E. no dispone de un procedimiento para la tramitación de los derechos de acceso, rectificación o cancelación en los términos establecidos

por la Ley Orgánica 15/1999, ya que una vez efectuadas las tareas de captura de la información de los cuestionarios en papel o a través de Internet, se procedió a la disociación de los datos identificativos de los censales y, por ello, no es posible el ejercicio de estos derechos previsto en dicha norma.

Creación de ficheros de titularidad pública

El fichero que contiene los datos correspondientes al Padrón Municipal de Habitantes a nivel nacional, cuya gestión y coordinación le corresponde al I.N.E. se encuentra inscrito en el Registro General de Protección de Datos con el código 2031700196.

Respecto a los ficheros censales al no contener datos de carácter personal no es de aplicación el precepto de su inscripción en el Registro General de Protección de Datos.

Movimiento internacional de datos

Los organismos internacionales solicitan periódicamente información de los diferentes países para elaborar estadísticas demográficas y sociales, siendo el *Censo Demográfico* una de las principales fuentes utilizadas. La Ley de la Función Estadística Pública no trata explícitamente la confidencialidad de los datos estadísticos en las relaciones internacionales.

Sin embargo, la Ley Orgánica de Protección de Datos en el artículo 33.1 prevé que «*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 la autorización previa del Director de la Agencia de Protección de Datos*». Lo dispuesto anteriormente no será de aplicación si la transferencia corresponde a la aplicación de tratados o convenios en los que sea parte España o cuando tenga por destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, en virtud de los apartados a) y k) del artículo 34 de dicha norma.

En este sentido, el Reglamento nº 1588/1990 del Consejo, relativo a la transmisión a la Oficina de Estadística de las Comunidades Europeas (EUROSTAT) de las informaciones amparadas por el secreto estadístico establece en el artículo 3 que, «*Las autoridades nacionales no estarán obligadas a transmitir a EUROSTAT las informaciones relativas a la vida privada de las personas físicas, cuando las informaciones transmitidas pudieran permitir la identificación directa o indirecta de tales personas*».

De las actuaciones efectuadas por parte de la Inspección de Datos en el ámbito de los *Censos de Población y Viviendas 2001* no se ha constatado que el I.N.E. hubiera facilitado datos personales a terceros que implicarán una transferencia internacional de datos.

Medidas de seguridad de los Sistemas de Información

Mediante Real Decreto 996/1999, de 11 de junio, se aprobó el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, que deberán ser adoptadas por el responsable del fichero y, en su caso, por el encargado del tratamiento.

Se ha comprobado que las compañías que han participado en la prestación de servicios en el ámbito de los *Censos de Población y Viviendas 2001* disponían de un documento en el que se especifican los aspectos relacionados con las medidas de seguridad implementadas en los Sistemas de Información tratados en el ámbito del Proyecto.

Por otra parte, el I.N.E. elaboró un documento en el que figuraban las medidas de seguridad que fueron implementadas en el Centro de Producción donde se realizó la captura de la documentación censal y la generación de los ficheros finales. Las medidas adoptadas fueron las calificadas como de nivel alto, ya que de la información que contenía el *cuestionario hogar* se podrían deducir datos calificados como especialmente protegidos de acuerdo con lo establecido en el artículo 7 de la Ley Orgánica 15/1999.

El I.N.E. dispone de un documento «*Padrón Continuo. Documento de Seguridad*» en el que se recogen las medidas de índole técnica y organizativas que el citado Instituto tiene implementadas en el Sistema de Información del Padrón con objeto de garantizar la seguridad de los datos de carácter personal contenidos en el mismo.

Conclusiones a las empresas participantes

De las actuaciones realizadas por parte de la Inspección de Datos y del análisis de la documentación recabada en las compañías que colaboraron en el desarrollo del Proyecto *Censos de Población y Viviendas 2001* se desprenden las siguientes conclusiones:

Deber de secreto

El I.N.E. elaboró el documento denominado «*Declaración de Empresa en Materia de Secreto Estadístico*», que debía ser preceptivamente suscrito por las empresas que colaboran en los *Censos de Población y Viviendas 2001*, en el que declaraban «*Haber leído y comprendido*» el contenido de su reverso en el que figuraban informaciones sobre «*El secreto esta-*

dístico», «*Las obligaciones que impone*» y «*Las consecuencias de su vulneración*». La empresa también se comprometía a que únicamente el personal que hubiera firmado el documento denominado «*Declaración Individual en Materia de Secreto Estadístico*» iba a participar en el trabajo contratado, debiendo entregar al Instituto Nacional de Estadística dichas declaraciones individuales.

La Inspección de Datos verificó que todas las compañías investigadas habían suscrito el documento «*Declaración de Empresa en Materia de Secreto Estadístico*», así como que los trabajadores pertenecientes a las mismas que estaban participando en el Proyecto habían firmado la «*Declaración Individual en Materia de Secreto Estadístico*». Sin embargo, se ha detectado que en los contratos que suscriben los trabajadores con las empresas no constan aspectos relativos a la obligación de guardar secreto respecto de los datos de carácter personal que conozcan en el desarrollo de sus funciones. Así mismo, se ha constatado que algunas de las empresas auditadas no informan a los trabajadores de la normativa relacionada con protección de datos y de las medidas de seguridad que deben cumplir las personas con acceso a ficheros automatizados que contengan datos de carácter personal.

Acceso a los datos por cuenta de terceros

Del análisis de la documentación contractual suscrita por las empresas se ha observado que en algunos Pliegos de Cláusulas Administrativas figuran como obligaciones del adjudicatario que:

a) *«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*».

b) *«Una vez finalizados los trabajos, 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 alguno de los Pliegos de Prescripciones Técnicas 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, se exige que la oferta deba «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 la información de carácter estadístico, regulada por la Ley 12/1989, de la Función Estadística Pública».*

De otro lado, hay que hacer especial mención a que, en determinados servicios las compañías adjudicatarias de los concursos públicos han tenido que subcontratar parte de los trabajos, ya que no podían cumplir con los plazos legales establecidos por el responsable del fichero, debido al volumen y complejidad de los trabajos a realizar. Por ello, suscribieron un contrato con el I.N.E. por el que el citado Organismo autorizaba a subcontratar en cumplimiento del artículo 12 de la Ley Orgánica 15/1999.

Medidas de Seguridad

Mediante Real Decreto 996/1999, de 11 de junio, se aprobó el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, que deberán ser adoptadas por el responsable del fichero y, en su caso, por el encargado del tratamiento.

Se ha comprobado que las compañías que han participado en la prestación de servicios en el ámbito de los *Censos de Población y Viviendas 2001* han elaborado un documento en el que se especifican los aspectos relacionados con las medidas de seguridad implementadas en los Sistemas de Información.

Las medidas adoptadas por las empresas han sido las calificadas como de nivel básico conjuntamente con las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20 del Reglamento de Medidas de Seguridad, ya que los ficheros podrían contener datos personales suficientes para obtener una evaluación de la personalidad del individuo. Por otra parte, las compañías que han tratado datos personales recabados de los cuestionarios cumplimentados por los ciudadanos han implementado las medidas de seguridad de nivel alto, ya que de la información que contenía el *cuestionario hogar* se podrían deducir datos calificados como especialmente protegidos de acuerdo con lo establecido en el artículo 7 de la Ley Orgánica 15/1999.

También se ha observado que para poder desempeñar las actividades establecidas en los contratos las empresas debían intercambiar información con el órgano contratante o con otros intervinientes en el Proyecto. Dichos intercambios de información se realizaron en soporte magnético o a través de medios telemáticos como Internet. A este respecto debe señalarse que, en algunos casos, la información no había sido cifrada ni se había utilizado otro medio que garantizará que no fuera inteligible ni manipulada durante su transporte.

3. Actuaciones más relevantes en el ámbito de los Ficheros de Titularidad Pública

3.1. Administración General del Estado

Algunos de los Sistemas de Información cuya titularidad corresponde a distintos órganos de la Administración General del Estado pueden considerarse de gran trascendencia y repercusión para los ciudadanos debido a su naturaleza, características y colectivo al que afectan y son, por tanto, de gran interés desde el punto de vista de protección de datos. Sin embargo, debemos destacar, como en años anteriores, el reducido número de quejas formuladas ante la Agencia de Protección de Datos por personas que han comunicado una vulneración de los principios establecidos en la Ley Orgánica 15/1999, por parte de las instituciones que integran dicha Administración.

Durante el año 2002 se han recibido en la Agencia de Protección de Datos un total de 57 quejas relacionadas con organismos de la Administración General del Estado, que han dado origen a la apertura de 34 actuaciones de investigación previa y, en el caso, de 23 de ellas a la tramitación de los correspondientes procedimientos de Tutela de Derechos. En cuanto a estos últimos, la Resolución del Director de la Agencia estimó la reclamación formulada en trece de ellas, desestimó la reclamación en cuatro de ellas, dándose traslado a la Agencia de Protección de Datos de la Comunidad de Madrid de una de ellas, y quedando pendiente de tramitación el resto de los procedimientos para el próximo ejercicio.

Las instituciones sobre las que se han centrado las actuaciones de investigación previa motivadas por quejas de los ciudadanos han sido las siguientes:

- La Tesorería General de la Seguridad Social.
- La Agencia Estatal de Administración Tributaria.
- La Dirección General de la Guardia Civil.
- El Instituto Nacional de Estadística.
- La Universidad Nacional de Educación a Distancia.
- La Mutualidad General de Funcionarios Civiles del Estado.
- El Instituto de Crédito Oficial.
- La Dirección General de Instituciones Penitenciarias.
- El Ministerio de Agricultura, Pesca y Alimentación.

De las 34 actuaciones previas iniciadas, en el caso de ocho de ellas se procedió al archivo de las mismas al no haberse constatado la existencia de infracciones a lo establecido en la normativa vigente sobre protección de datos. De las restantes, en unos

casos, se procedió a la apertura de procedimientos de infracción de las Administraciones Públicas, o bien, se encuentran pendientes de finalización de las oportunas investigaciones.

3.1.1. *Resoluciones más relevantes dictadas en relación con la Administración General del Estado*

El Director de la Agencia de Protección de Datos ha dictado, durante el ejercicio 2002, once resoluciones de procedimientos de infracción de las Administraciones Públicas referidas a Instituciones u Órganos encuadrados en la Administración General del Estado, algunos de los cuales se habían iniciado en el ejercicio anterior. Cabe destacar que, de las once resoluciones resueltas, en nueve de ellas se concluyó que se había vulnerado lo dispuesto en la Ley Orgánica 15/1999. A continuación se citan aquellas resoluciones que requieren una especial mención:

Tesorería General de la Seguridad Social

En primer lugar se debe indicar que cinco resoluciones sancionadoras de procedimientos de infracción de las Administraciones Públicas corresponden a la Tesorería General de la Seguridad por haber infringido, en unos casos, lo dispuesto en el artículo 10 y, en otros, lo dispuesto en el artículo 4.2 de la Ley Orgánica 15/1999, lo que supone una infracción tipificada como grave en los artículos 44.3 g) y 44.3 d) respectivamente de la citada norma. Dichas infracciones han estado relacionadas con el tratamiento de datos de carácter personal incluidos en el Sistema de Información, denominado «*afiliación*», que contiene datos personales de millones de trabajadores y al que tienen acceso diversas instituciones de las Administraciones Públicas. Los datos personales obtenidos vulnerando los principios de protección de datos han sido facilitados, por terceros, al Juzgados o Tribunales en el ámbito de procedimientos judiciales, y a medios de comunicación.

Las resoluciones por vulneración del deber de secreto indican que ha quedado acreditado que ha sido facilitada a terceros información relativa a la vida laboral de los afectados sin contar con su consentimiento. La citada información recoge aspectos como: el nombre y apellidos del afectado, su número de afiliación a la Seguridad Social, D.N.I., fecha de nacimiento, grupo y periodos de cotización a la Seguridad Social con indicación de la empresa, fecha de alta y fecha de baja, siendo dicha información fiel reflejo de la contenida en el fichero de afiliación de la Tesorería General de la Seguridad Social.

Asimismo, en la tramitación de los procedimientos el propio Organismo ha informado que los accesos a los datos de los afectados no están justificados, mediante la correspondiente documentación acreditativa necesaria para la solicitud de dicha información por parte del

afectado, y que tampoco han sido efectuados en el ámbito de las funciones que normativamente tiene encomendadas la institución.

La Tesorería General de la Seguridad Social ha alegado en la tramitación de los procedimientos de infracción de Administraciones Públicas que los hechos que se le imputan constituyen la infracción leve descrita en el artículo 44.2 e), y no la infracción grave definida en el artículo 44.3 g), dado que la información que consta en sus ficheros no puede servir para obtener una evaluación de la personalidad del individuo. No obstante, esta alegación ha sido rechazada porque conocer la vida laboral de una persona (fechas de altas y bajas, motivos de las bajas, entidades contratantes, calificación profesional, etc.) conjuntamente con datos identificativos, sí ofrece una información necesaria y útil para establecer un perfil del individuo. La evaluación de una personalidad también se obtiene atendiendo a la vida laboral del sujeto en cuestión, pues a través de los datos que obran en el fichero de la Tesorería, se puede conocer la actividad profesional que ha realizado o que realiza la persona consultada, así como las entidades en las que ha prestado sus servicios y el tiempo de duración de la relación contractual.

Así mismo, en las resoluciones sancionadoras de los procedimientos de Administraciones Públicas se propone a la Tesorería General de la Seguridad Social que inicie las actuaciones disciplinarias oportunas contra los funcionarios responsables de los hechos que vulneran la normativa de protección de datos.

Con respecto a las resoluciones sancionadoras por vulneración del artículo 4.2 de la Ley Orgánica 15/1999, que 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*», la conducta que se considera contraria a la citada norma consiste en la consulta injustificada por parte de funcionarios habilitados de la Tesorería General de la Seguridad Social de datos personales, contenidos en los ficheros de la mencionada entidad, sin que los accesos estén justificados, pues no se realizaron como consecuencia del trabajo habitual ni obedecen a principios y objetivos de gestión.

La Tesorería General de la Seguridad Social alega en la tramitación del procedimiento que la presunta vulneración a la Ley Orgánica de Protección de Datos cometida por los funcionarios no puede implicar responsabilidad alguna del Organismo, ya que, si bien dichos funcionarios están facultados para utilizar las transacciones informáticas que acceden al fichero «*afiliación*», su actuación injustificada obedece a una cuestión particular de los mismos, por lo que la Tesorería, como responsable del fichero, actuó con la debida diligencia garantizando la seguridad de los datos.

Habida cuenta de los preceptos recogidos en la Ley Orgánica, como el artículo 3.d) que dispone que se entenderá por responsable del fichero al órgano administrativo y el artículo 43

que establece que los responsables de los ficheros estarán sujetos al régimen sancionador establecido en dicha norma, la alegación invocada no prosperó, pues el responsable del fichero del que se obtuvieron los datos es la Tesorería General de la Seguridad Social y, el régimen sancionador es de exclusiva aplicación al responsable del fichero, sin perjuicio, de las responsabilidades que, en su caso, se estimen oportuno exigir a los funcionarios responsables. En tal sentido, la Resolución señala que el artículo 46 de la precitada norma, «Infracciones de las Administraciones Públicas», en su punto 2, dispone que «*El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas*». Dichas actuaciones han sido propuestas a la Tesorería General de la Seguridad Social por parte del Director de la Agencia de Protección de Datos en las resoluciones sancionadoras.

Universidad Nacional de Educación a Distancia

La Resolución del Director de la Agencia de Protección declara que la Universidad Nacional de Educación a Distancia ha infringido lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999, por comunicación de datos de carácter personal de sus alumnos sin consentimiento de éstos para fines publicitarios, y lo dispuesto en el artículo 9 de dicha norma, en relación con los artículos 8, 11 y 12 del 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, lo que supone una infracción tipificada como muy grave en los artículos 44.4 b) y 44.3 h), respectivamente, de la citada norma.

Durante la tramitación del procedimiento quedó acreditado que el envío publicitario recibido por el denunciante, en el que ofertaba productos de dos empresas, tenía por destinatarios alumnos de la Universidad Nacional de Educación a Distancia. Si bien, no ha podido concretarse el método de obtención de los datos de los destinatarios por parte de la empresa encargada de la campaña publicitaria, no es menos cierto que no existen dudas respecto de los destinatarios de la misma. En este sentido la propia Universidad reconoce que algún representante de alumnos facilitó 150.000 direcciones de alumnos a dicha empresa. La Resolución señala que dicha comunicación de datos fue realizada sin conocimiento de los órganos de gobierno de la Universidad o de los directores de las respectivas Facultades, aunque ello no implica que no se deba imputar a dicha institución la responsabilidad de la cesión de datos personales de sus alumnos sin el consentimiento previo de los interesados y sin existir ninguna causa de exclusión del consentimiento de las previstas en el artículo 11.2 de la Ley Orgánica 15/1999.

Según la Resolución los ficheros de la Universidad Nacional de Educación a Distancia relativos a su alumnado deben tener implantadas las medidas de seguridad de nivel alto. No obstante, dado que a la fecha de inicio del presente procedimiento aún no eran exigibles las

medidas de seguridad del referido nivel, se imputó a la citada Universidad el incumplimiento de medidas de nivel básico y, en concreto, la ausencia de documento de seguridad y la inexistencia de la relación actualizada de los usuarios que tengan acceso autorizado al Sistema de Información, según lo establecido en el Reglamento de Medidas de Seguridad citado.

Instituto Nacional de la Seguridad Social

El Director de la Agencia de Protección resuelve que el Instituto Nacional de la Seguridad Social ha infringido lo dispuesto en el artículo 10 de la Ley Orgánica 15/1999, por facilitar datos personales de un pensionista a terceros sin su consentimiento, lo que supone una infracción tipificada como grave en el artículo 44.3 g) de la citada norma.

El Instituto Nacional de la Seguridad Social ha accedido a los datos económicos de pensión del afectado y generado el certificado en el que constan datos identificativos, clase de pensión (incapacidad absoluta), régimen, fecha de efectos, suma de abonos, etc., sin que quede constancia de haberse aportado la documentación necesaria para solicitar dicho documento. El Organismo tiene establecido que para facilitar este tipo de información se requiere al solicitante el original del D.N.I., con independencia de que sea el titular. En el caso de no aportar dicho documento, la solicitud se realiza por escrito con fotocopia del D.N.I. del titular y del representante y el certificado se remite por correo certificado al domicilio que consta en los Sistemas de Información de dicho Instituto. En el caso analizado, no existía documento acreditativo de la solicitud del certificado de pensionista ni del envío por correo del mismo al domicilio del titular de los datos personales.

La información contenida en el certificado fue revelada a persona distinta del interesado, sin que haya sido solicitada por el Órgano Judicial ante el que se presentó. Por todo ello, se declara que el Instituto Nacional de la Seguridad Social ha incumplido las normas establecidas de protección de datos de carácter personal, vulnerando el deber de secreto profesional de los datos personales que debe guardar el responsable del fichero y quienes intervengan en cualquier fase del tratamiento.

Instituto Nacional de Empleo

Por Resolución del Director de la Agencia de Protección de Datos se declara que el Instituto Nacional de Empleo ha infringido lo dispuesto en el artículo 10 de la Ley Orgánica 15/1999, por facilitar datos personales del contrato de trabajo de la afectada a un tercero sin su consentimiento, lo que supone una infracción tipificada como grave en el artículo 44.3 g) de la citada norma.

En este caso, quedó acreditado que el Instituto Nacional de Empleo facilitó a terceras personas, mediante la expedición de un documento interno, información sujeta al deber de

secreto relativa al contrato de trabajo de la afectada, datos que permiten obtener una evaluación de la personalidad de su titular. Copia de dicho documento se aportó posteriormente como prueba en un Juzgado, siendo rechazada su estimación de conformidad con lo establecido en el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, al ser contraria su obtención al artículo 18.4 de la Constitución Española, al no constar autorización de la interesada para disponer de aquella información personal relativa a su contrato, ni haberse obtenido a requerimiento del órgano judicial. Dichas circunstancias constan en la Sentencia que, de oficio, trasladó el Juzgado a esta Agencia de Protección de Datos para que se realizaran las averiguaciones oportunas por si los hechos pudieran ser constitutivos de infracción a la Ley Orgánica 15/1999.

Entidad Pública Empresarial Correos y Telégrafos

La Resolución del Director de la Agencia de Protección declara que la Entidad Pública Empresarial Correos y Telégrafos ha infringido lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999, por ceder datos personales de sus empleados a tercera entidad sin recabar el consentimiento de los afectados, lo que supone una infracción tipificada como muy grave en el artículo 44.4 b) de la citada norma.

La Dirección Provincial de Correos y Telégrafos de La Rioja cedió los datos personales de los empleados de dicha entidad que constan en sus ficheros automatizados y, en particular los del afectado, a una empresa sin el previo consentimiento de los afectados y fuera de los casos enumerados en el artículo 11.2 de la Ley de Protección de Datos de Carácter Personal. La información facilitada por Correos y Telégrafos fue entregada en un listado que contenía los nombres, apellidos y lugar de trabajo de sus empleados, con la finalidad de realizar un mailing promocional a los empleados de la entidad.

El artículo 11 de la Ley Orgánica 15/1999, 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 legítimas del cedente y del cesionario con el previo consentimiento del interesado*». Dicho precepto ha sido analizado por la STS de 31 de octubre de 2000, donde se sostiene que el citado artículo exige concurrencia de tres notas para que se proceda a la cesión: *«consentimiento previo del afectado...; que la cesión se relacione con el cumplimiento de los fines del cedente...; que la cesión se relacione también con los fines del cesionario».* En el caso enjuiciado no concurren cumulativamente los requisitos apuntados al carecer del consentimiento del afectado, pues los datos fueron recabados de los ficheros automatizados de Correos y Telégrafos y, posteriormente, cedidos en soporte papel a tercera entidad, no se cumple la función legítima del cedente al haberse realizado la cesión con una finalidad promocional incompatible con la función que le es propia y en beneficio de la tercera entidad que realizó el mailing promocional.

3.2. Administraciones Autonómicas

Durante el ejercicio 2002 destacan dos resoluciones dictadas en el ámbito de las administraciones autonómicas:

- La primera de ellas declaró que la Universidad de Granada había infringido el artículo 11.1 de la Ley Orgánica 13/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por haber cedido los datos de los estudiantes de segundo ciclo a una Fundación sin el consentimiento expreso de los estudiantes. La Resolución declaró que la Universidad de Granada, en calidad de responsable del fichero, debió asegurarse de que contaba con el consentimiento previo de los afectados sin exceptuar esta obligación la relación de la Universidad de Granada con la Fundación ni el hecho de que en su Consejo esté presente el Rector de la Universidad de Granada, pues ambas son entidades distintas que actúan en nombre propio en sus actividades docentes.

  La Resolución instó a la Universidad de Granada a que adoptara las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 11.1 de la Ley Orgánica 15/1999.

- La segunda de ellas declaró que la Consejería de Educación y Juventud del Gobierno de Cantabria infringió lo dispuesto en el artículo 10 de la Ley Orgánica al suministrar a *El Diario Montañés* unas pruebas de impresión de títulos académicos entre los que aparecían los datos de carácter personal de la denunciante, infringiendo el de deber de confidencialidad que obliga no solo al responsable del fichero sino a todo aquel que intervenga en cualquier fase de tratamiento.

  En la misma se requirió a la Consejería de Educación y Juventud del Gobierno de Cantabria, a que tomara las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de dicho artículo.

Por otra parte, durante el año 2002 se procedió a la apertura por parte de la Inspección de Datos de catorce actuaciones previas de investigación relacionadas con el posible incumplimiento de lo establecido en la Ley Orgánica 15/1999 por parte de los responsables de ficheros pertenecientes al ámbito de diversas Comunidades Autónomas así como siete procedimientos de Tutela de Derechos.

Cuatro de las actuaciones previas de Inspección terminaron antes del final del ejercicio, tres de ellas con el archivo de las actuaciones y una con la apertura de un procedimiento sancionador de Administraciones Públicas a la Junta de Castilla La Mancha, procedimiento que no había finalizado al término del ejercicio.

Entre las tres actuaciones archivadas están las actuaciones practicadas por la Agencia de Protección de Datos en la Consejería de Bienestar Social de la Junta de Castilla-La Mancha ante la noticia aparecida en diversos medios de comunicación social de que el Gobierno de Castilla-La Mancha había hecho pública una lista de dieciocho sentencias firmes condenatorias sobre la violencia doméstica.

Durante las actuaciones previas llevadas a cabo por la Inspección de Datos se constató que la Consejería citada había elaborado un Informe anual recogiendo dicha información, en cumplimiento de la Ley 5/2001, de 17 de mayo, de prevención de malos tratos y protección a las mujeres maltratadas y del Decreto 38/2002, de 12 de marzo, que la desarrolla.

En dicho Informe se incluyeron 18 sentencias firmes condenatorias sobre violencia doméstica elaborándose un Resumen del Informe en el que también se incluyeron dichas sentencias.

En la materialización del Informe y del Resumen se omitieron los datos identificativos de las personas intervinientes a excepción del nombre y apellidos del condenado que sí se hizo constar en los párrafos finales de las sentencias donde se recoge el fallo, manteniendo, en algunos casos, la localidad de residencia de los implicados.

La publicación de las sentencias se hizo con la autorización de las víctimas.

En ningún caso los datos de carácter personal de los denunciados o condenados por malos tratos fueron incorporados a los ficheros automatizados de la Consejería.

El Director de la Agencia de Protección de Datos resolvió que los citados hechos quedaban al margen del ámbito de aplicación de la Ley Orgánica 15/1999, toda vez que la publicación de dichas sentencias se realizó en soporte físico no susceptible de tratamiento automatizado posterior, ni estructurado de forma que permita acceder al contenido del mismo tanto mediante técnicas automatizadas como manuales, y en consecuencia, no acorde con la definición de fichero dada por la citada LOPD.

3.3. Administración Local

Durante el año 2002, se han resuelto 65 procedimientos de infracción de Administraciones Públicas por vulneración de la Ley Orgánica 15/1999 iniciados por tratamientos realizados por parte de entidades pertenecientes a la Administración Local, en su gran mayoría Ayuntamientos. De las resoluciones dictadas 64 han sido sancionadoras.

Cabe destacar que de las mencionadas resoluciones sancionadoras 58 han sido como consecuencia de los procedimientos de infracción de Administraciones Publicas incoados

a otros tantos Ayuntamientos por infracción del artículo 20 de la Ley Orgánica 15/1999, tipificada como grave en el artículo 44.3.k) de dicha norma que considera como tal *«no inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos».*

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 con una población superior a cuatro mil habitantes, para el cumplimiento de la obligación de notificación de los ficheros que contengan datos personales de los cuales fueran responsables. En todos los casos ha quedado acreditado que el Ayuntamiento correspondiente no ha procedido a inscribir dichos ficheros en el Registro General de Protección de Datos, a pesar de haberle sido requerido tal extremo en varias ocasiones.

Del resto de las resoluciones sancionadoras, dos de ellas han sido por infracción de lo dispuesto en artículo 11 de la Ley Orgánica, 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».* En los dos casos ha quedado probado que por parte de dos entidades de la administración local se facilitaron datos procedentes de sus ficheros a entidades privadas tras haber realizado un acuerdo verbal con las mismas para la prestación de un servicio, sin haber cumplido los requisitos establecidos en el apartado 2º del art. 12 de la Ley Orgánica que especifica 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 de 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*»...».

También resulta interesante mencionar la resolución sancionadora que se dicta como consecuencia del incumplimiento de lo dispuesto en el artículo 4.2 de la LOPD, que establece: «*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos 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 dicho caso quedó probado que el Ayuntamiento en cuestión utilizó los datos del «Padrón Municipal de Habitantes», para el envío a algunos vecinos de la localidad, de una información relacionada con la visita

del Alcalde del Municipio a otro Municipio. En las alegaciones presentadas por el Ayuntamiento éste consideraba que al ser el Padrón Municipal de Habitantes un registro de población, es un instrumento de comunicación con los ciudadanos, que en este caso se utilizó en el ejercicio de sus funciones para favorecer la integración social de sus vecinos, nacidos en otro Municipio. En la Resolución se pone de manifiesto que la Agencia de Protección de Datos no prohíbe, ni puede prohibir que un Ayuntamiento tenga una política activa de integración social, pero sí tiene que velar por el cumplimiento de la normativa de protección de datos de carácter personal. En este sentido, la normativa que regula el Padrón Municipal de Habitantes es estricta en cuanto a las finalidades del tratamiento de datos y su utilización.

El Padrón Municipal de habitantes es un registro de población de naturaleza administrativa, donde constan los vecinos del municipio y constituye elemento probatorio a efectos de acreditación de la residencia en el municipio y del domicilio de los vecinos. Así mismo, de conformidad con lo establecido en el artículo 16.1 de la Ley de Bases de Régimen Local, la expresión *«Datos del Padrón Municipal»* se refiere 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. La utilización de los datos del Padrón de Habitantes con una finalidad diferente se rige por lo dispuesto en la normativa de Protección de Datos de Carácter Personal, requiriendo el consentimiento de los afectados para su tratamiento.

Respecto a las actuaciones iniciadas en el año anterior, tras la aparición en los medios de comunicación de una noticia relativa a la posible utilización por parte de la Policía Local de dos Ayuntamientos, de expedientes sobre datos policiales de los ciudadanos, el Director de la Agencia dictó sendas resoluciones de archivo de las actuaciones realizadas por la Inspección de Datos dado que ha quedado probado que los datos personales de los detenidos en los citados Municipios eran incorporados en los dos casos a un fichero manual preexistente a la entrada en vigor de la Ley Orgánica 15/1999, sin existir fichero automatizado para la gestión del servicio por lo que, según establece la Ley Orgánica en su disposición Adicional Primera, *«Ficheros Preexistentes»,* párrafo segundo «*En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados....*».

Sin embargo, en relación con el mismo fichero manual de uno de los dos Ayuntamientos, se ha dictado otra resolución en este caso sancionadora, por infracción de lo dispuesto en el art. 16 de la Ley Orgánica, relativo a los derechos de rectificación y cancelación, como consecuencia de una Tutela de Derechos iniciada con motivo de una reclamación inter-

puesta contra el mismo Ayuntamiento por no haber atendido éste una solicitud de cancelación. En dicho caso se acreditó que a pesar de que la Comisión de Gobierno del Ayuntamiento acordó cancelar todos los antecedentes registrados con fines policiales en la Jefatura de Policía Local referidos a un ciudadano, casi un año después se conservaban en las citadas dependencias policiales dos expedientes personales relativos al denunciante que contenían las anotaciones policiales que se hubieran debido cancelar.

Así mismo, de las actuaciones de Inspección finalizadas a lo largo del año 2002 en relación con tratamientos efectuados dentro del ámbito de la Administración Local, ocho de ellas han dado lugar a otras tantas resoluciones de archivo de actuaciones, en dos de los casos, por tratarse, así mismo de tratamientos de datos contenidos en ficheros manuales preexistentes a la entrada en vigor de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

3.4. Fuerzas y Cuerpos de Seguridad del Estado

Bajo esta rúbrica se hará referencia a alguna de las actuaciones desarrolladas en el ámbito del Convenio de Schengen, así como a la denominada Operación Ludeco, de la Dirección General de la Policía.

3.4.1. *Actuaciones relacionadas con el Convenio Schengen*

Como en años anteriores, 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, cuyos datos habían sido introducidos por las autoridades españolas.

En todos los casos, se iniciaron las actuaciones pertinentes con el fin de verificar si los datos de dichas personas habían sido incluidos correctamente al amparo de la legislación vigente. Como consecuencia de las mismas se realizaron inspecciones sobre los ficheros y archivos de la Comisaría General de Extranjería y Documentación de la Dirección General de la Policía, comprobando que dichas personas habían sido expulsadas del territorio nacional tras la incoación de un expediente de expulsión de conformidad con la Ley Orgánica 4/2000 de 11 de enero, de Extranjería, decretándose la prohibición de

entrada en el país. Culminadas las investigaciones se informó a la CNIL de las actuaciones realizadas, así como del motivo por el que figuraban dichas personas incluidas en el SIS.

3.4.2. *Operación Ludeco*

En el año 2001 la Dirección General de la Policía puso en marcha la Operación LUDECO, con la publicación de una Circular en fecha 19/10/2001 de la Subdirección General Operativa. Esta 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. En la comparecencia del Director de la Agencia ante la Comisión Constitucional del Congreso de los Diputados que tuvo lugar el 7 de noviembre de 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, motivo por el que decidió la realización de actuaciones de inspección de oficio, que culminaron en el año 2002.

La inspección realizada analizó las medidas adoptadas en el ámbito de la inteligencia criminal, en la aplicación de la normativa en materia de extranjería y en la cooperación internacional, con objeto de verificar que los tratamientos de datos personales aplicados no suponían una criminalización de los extranjeros contraria al sistema de garantías de la LOPD.

En el ámbito de la inteligencia criminal se inspeccionó el fichero GATI al que se hacía referencia en la Circular citada. Este fichero incluye información relacionada con investigaciones criminales, conteniendo dos bases de datos denominadas INVESTIGA Y ARCHIVA. Con el fin de comprobar si existía un tratamiento indiscriminado y generalizado de datos de ecuatorianos y colombianos se realizó un análisis cuantitativo de los que figuraban en las dos bases de datos mencionadas. Los datos obtenidos pusieron de manifiesto que el total de nacionales colombianos y ecuatorianos incluidos en el GATI, constituían un porcentaje reducido respecto del total de personas incorporadas en dicho fichero (el porcentaje más elevado se producía en el fichero INVESTIGA y ascendía al 4,1%). De dicho colectivo sólo estaban afectados por la OPERACIÓN LUDECO un 10,84% en el caso del fichero INVESTIGA y un 1,79% en el de ARCHIVA.

De las verificaciones realizadas se desprende que el fichero GATI no tiene como finalidad el tratamiento generalizado e indiscriminado de nacionales ecuatorianos y colombianos, así como que el tratamiento de datos derivados de la Operación LUDECO afecta a un porcentaje reducido de nacionales ecuatorianos y colombianos que son objeto de investigaciones criminales.

También se comprobó que el fichero tenía un Registro Control de Accesos para detectar accesos indebidos. En particular, se constató que los servicios administrativos encargados de la tramitación de los permisos de residencia no tenían acceso al fichero GATI. Ello supone que están implantadas las medidas adecuadas para garantizar los principios de finalidad y seguridad en el tratamiento de los datos.

Por otra parte, se realizaron actuaciones inspectoras en el Registro Central de Extranjeros correspondiente al fichero denominado EXTRAN. Su objetivo fue constatar si se producía o no un trasvase generalizado de datos desde el fichero EXTRAN al fichero GATI. De las comprobaciones realizadas se desprende que los datos de las personas a las que se había otorgado el permiso de residencia no estaban incluidos en el fichero GATI y que los datos de personas a las que se había denegado el permiso de residencia y cuyos datos fueron incorporados al fichero GATI, correspondían a aquellas que contaban con antecedentes policiales o penales. De estas comprobaciones se deducía que no existía un trasvase de datos generalizado entre ambos ficheros.

En el ámbito de la cooperación internacional se comprobó que los intercambios de información con organismos policiales de otros países se encontraban amparados en diversos Instrumentos internacionales suscritos por España.

3.5. 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 Agencia por su adecuación a las prescripciones legales. Entre las resoluciones más significativas dictadas durante el año 2002, respecto del tratamiento de datos de salud, cabe destacar las siguientes:

Inexistencia de algunas medidas de seguridad en un Hospital perteneciente al Servicio Andaluz de Salud

En el año 2001 se recibió una reclamación contra un Hospital dependiente del Servicio Andaluz de Salud, en base a la documentación presentada en una demanda civil seguida contra la hija del denunciante a la que se acompañaban como prueba, documentos relativos a su salud provenientes del citado hospital. Estos documentos se correspondían con copias de certificaciones expedidas por dicho Hospital relativas al parto de la interesada así como copias de su historial clínico.

Como consecuencia de las actuaciones inspectoras se determinó que el Hospital no disponía de un registro de auditoria que permitiera conocer quién accedió a los sistemas infor-

máticos al objeto de extraer una copia de la historia clínica relativa a la hija del denunciante, hecho por el cual se inició un procedimiento sancionador contra el Hospital que se resolvió declarando que éste había cometido una infracción del artículo 9 de la LOPD que exige la adopción de medidas de seguridad en el tratamiento de datos personales, tipificada como grave en el artículo 44 de dicha norma.

Utilización con fines particulares de los datos de un paciente, realizada por un médico del Centro de Salud que le atendía

En la Memoria relativa al año 2001 se informó de una reclamación sobre la cual no se había dictado resolución, en la que se denunció a un determinado Centro de Salud del INSALUD ubicado en la Comunidad de Madrid 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.

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. Sin embargo, dado que en diciembre de 2001 se traspasaron a la Comunidad de Madrid las funciones y servicios del Instituto Nacional de la Salud, el Director de la Agencia acordó el traslado del procedimiento con toda la documentación, a la Agencia de Protección de Datos de la Comunidad de Madrid.

Aportación de análisis clínicos de pacientes en un expediente disciplinario abierto a una trabajadora hospitalaria

La denunciante pone de manifiesto que siendo trabajadora de un hospital dependiente del Ministerio de Defensa, recibió un oficio de dicho hospital en el que le comunicaron la apertura de un expediente disciplinario. Al trasladarle la documentación obrante en el expediente, comprobó que figuraban copias de veintisiete resultados de análisis médicos realizados a otras tantas personas ajenas al expediente disciplinario, estimando que se había vulnerado la confidencialidad de las pruebas médicas.

Tras la realización de las actuaciones inspectoras pertinentes, se puso de manifiesto que el citado hospital abrió un expediente disciplinario a la denunciante, siendo uno de los motivos de incoación del mismo la posible falta de rigor en el resultado de algunos análisis clínicos de microbiología, así como el no entregar los resultados en la fecha inicialmente prevista. Como prueba de ello se incluyeron en el expediente copias de los resultados de los análisis clínicos correspondientes a veintisiete pacientes, en los que figuraban además de

los datos analíticos, los relativos a la identificación de los pacientes, entre ellos el número de historia, el nombre y los apellidos. Una vez concluida la tramitación del expediente, la afectada solicitó copia completa del mismo procediendo el Hospital a facilitarle lo solicitado. Los representantes del hospital manifestaron que la inclusión en el expediente disciplinario de los resultados analíticos se consideró necesaria como documento probatorio de los hechos que se imputaban a la trabajadora.

En la inspección realizada se comprobó que en el expediente disciplinario figuraba el sello de «*Confidencial*», y que entre la documentación que contenía se encontraba copia de veintisiete análisis correspondientes a veintisiete pacientes. Estos análisis figuraban en el fichero de análisis clínicos del Servicio de Microbiología del Hospital.

La reclamación fue archivada debido a que el expediente disciplinario que se instruyó a la denunciante, fue realizado siguiendo el procedimiento establecido en el Convenio Único para Personal Laboral de la Administración General del Estado. Por otra parte al aportar las copias de los resultados de los análisis clínicos realizados, se puso el sello de «*Confidencial*», con el fin de garantizar la intimidad de los pacientes.

4. Actuaciones más relevantes en el ámbito de los Ficheros de Titularidad Privada

4.1. Compañías de Telecomunicaciones

Durante el año 2002 se han dictado un total de veintiséis resoluciones relativas al sector de las telecomunicaciones. A continuación se recoge un extracto de las mismas agrupadas por temas, profundizando en aquellas que presentan un mayor interés desde el punto de vista jurídico.

4.1.1. *Inclusión de datos de clientes en ficheros de morosidad*

Del conjunto de resoluciones en el sector, diecisiete tienen su origen en denuncias como consecuencia de la inclusión por parte de las empresas de telecomunicaciones de datos de clientes en ficheros comunes de incumplimiento de obligaciones dinerarias regulados por el artículo 29 de la LOPD, como consecuencia de reclamaciones de cantidad.

Si bien las reclamaciones de cantidad presentan un origen variado, cabe señalar como principales motivos los siguientes: errores en los procesos de facturación, solicitudes de baja de

servicio no cursadas prolongándose la situación de alta, no proceder a la cancelación de la deuda tras el pago de la misma, atribución de la deuda de un cliente a otra persona al incluir en ficheros comunes de incumplimiento de obligaciones dinerarias datos identificativos erróneos y altas fraudulentas.

De estas diecisiete resoluciones, una terminó con el archivo de las actuaciones, mientras que las dieciséis restantes finalizaron con resoluciones sancionadoras, incurriendo la totalidad de estas últimas en faltas graves. En este sentido, es interesante señalar que, en la mayoría de los casos, las empresas sancionadas solicitaron el archivo de las actuaciones alegando que la inclusión de los datos de los afectados en ficheros de morosidad carecía del elemento de la culpabilidad, ya que se habían producido como consecuencia de errores informáticos o de procedimiento.

Frente a las alegaciones anteriores, y en base a los criterios mantenidos por los tribunales, la Agencia consideró que los responsables del tratamiento, que se sirven y benefician de estos ficheros comunes de morosidad, deben de extremar la diligencia a fin de evitar que, ya sea por negligencia o por incumplimiento de los deberes que la Ley les impone, ocasionen un perjuicio a un afectado, como es el de la inclusión indebida de sus datos en un fichero de este tipo.

A mayor abundamiento, hay que indicar que este grupo de resoluciones se centra sobre operadores que no son precisamente los que más clientes tienen, por lo que no se sostiene la argumentación de que se trata de errores inherentes al gran volumen de información manejada. En este sentido, puede decirse que el origen de estas actuaciones radica principalmente en deficiencias en los procedimientos de gestión establecidos por los operadores afectados.

4.1.2. *Repertorios de abonados o guías telefónicas*

Otro grupo lo constituyen cinco resoluciones dictadas en relación con los repertorios telefónicos de abonados conocidos habitualmente como *«guías».* De éstas, tres resoluciones tienen que ver con las denominadas guías inversas, u obtención de los datos personales de los abonados a partir del número de teléfono, una cuarta resolución se dictó como consecuencia del ejercicio del derecho a no figurar en la guía y una quinta en relación a la utilización de los datos recabados de las guías para fines de publicidad por parte de empresas de marketing directo.

Respecto de las guías inversas, la Agencia participa del criterio mantenido por el resto de Autoridades de control europeas recogido en la Opinión 5/2000, de 13 de julio, elaborada por el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. Según este criterio, el trata-

miento de los datos personales en guías que permiten la búsqueda inversa o multicriterio, es contrario a la normativa legal, si no se dispone del consentimiento informado del afectado.

A lo anterior, hay que añadir que con fecha de 26 de marzo, el Ministerio de Ciencia y Tecnología dictó la Orden CTE/11/2002 que prescribe la prohibición de las consultas sobre las guías telefónicas que permiten obtener la identidad o el domicilio de un abonado a partir de su número de teléfono u otro recurso identificativo del mismo, reiterando en una norma reglamentaria el criterio legal de que este tratamiento de los datos es contrario al principio de finalidad.

Lo expuesto, ha llevado a la Agencia a dictar las citadas tres resoluciones sancionadoras sobre guías inversas cuyo contenido se resume a continuación:

- En una primera se sancionó a una empresa española por elaborar y comercializar un producto en CD-ROM que contenía una guía de abonados telefónicos, con la funcionalidad añadida de poder realizar búsquedas inversas y multicriterio.

- En una segunda se sancionó a otra empresa española que distribuía un producto similar al anterior elaborado, en esta ocasión, por la empresa belga Kapitol.

- En una tercera resolución, se sancionó a una empresa española en cuya página *web* se facilitaba un servicio de guía inversa mediante la recogida, a través de su propia *web*, del número de teléfono a consultar, realizando seguidamente, una consulta sobre el servicio de guía telefónica inversa de la empresa belga Kapitol, quien finalmente facilita el resultado.

  En este caso, la empresa alegó en su descargo que la guía telefónica inversa era un simple vínculo, copiado y pegado de otra página *web* que sí albergaba dicha guía. No obstante, dicho alegato no fue tenido en cuenta por cuanto para acceder a la información de nombre y dirección, era preciso teclear el número de teléfono que se deseaba consultar en la propia página de la empresa sancionada.

  En relación con esta problemática, cabe señalar que durante el ejercicio de 2002 ha dejado de funcionar la funcionalidad de búsqueda inversa que, sobre abonados españoles, ofrecía a través de Internet la empresa Kapitol, ya citada anteriormente. El cierre de este servicio, pone fin a diversas quejas que habían sido formuladas ante esta Agencia, y como consecuencia de las cuales, se había instado la intervención de la Autoridad de Protección de Datos de Bélgica, por ser en este país donde radicaba la actividad de la citada empresa.

- Respecto de la cuarta resolución dictada en relación a la solicitud por un ciudadano de su exclusión de la guía, cabe señalar que, en este caso, el operador titular de la

guía atendió debidamente dicha solicitud de exclusión sobre la guía en soporte papel, no así, sobre la guía electrónica accesible a través de Internet debido a un problema de comunicación entre el operador y la empresa que gestiona la guía electrónica. Esta circunstancia ocasionó un perjuicio a la persona que lo denunció ya que, durante más de un año, su nombre apareció vinculado a un número de teléfono erróneo en esta última guía.

Lo relevante de este caso, radica en que el operador alegó que la exclusión de datos de la guía telefónica no constituye un derecho de cancelación, regulado en el artículo 16 de la LOPD, sino un derecho regulado en el artículo 28.4 de dicha norma, respecto del cual no existe un procedimiento reglamentario que desarrolle su ejercicio, no existiendo, por lo tanto, un plazo legal máximo establecido para su cumplimiento.

Frente a la alegación anterior, la Agencia mantiene el criterio de que la exclusión de datos de tales guías es una manifestación del derecho de cancelación en el repertorio de telecomunicaciones, por lo que considera que la solicitud de exclusión implica necesariamente el ejercicio de tal derecho, debiendo el responsable del fichero contestar expresamente a dicha solicitud, motivando, en su caso, la negativa a su aceptación en aplicación del artículo 16 de la LOPD, o bien haciendo efectivo el derecho en el plazo de diez días.

- Finalmente sobre el tema de guías, cabe señalar la quinta resolución sancionadora contra una empresa del sector de marketing directo que utilizaba los datos de dicho repertorio para el envío de publicidad por cuenta de sus empresas clientes.

A este respecto, hay que señalar que el artículo 30 de la LOPD permite a las empresas de marketing utilizar, con fines publicitarios, los datos obtenidos de fuentes accesibles al público, no siendo necesario para ello disponer del consentimiento del afectado.

A lo ya indicado por el artículo 30 hay que añadir lo apuntado por el artículo 28.3 de la misma Ley, que configura una limitación temporal al carácter de fuente accesible al público. Así, se establece que las fuentes accesibles al público que se editen en forma de libro, o algún otro soporte físico, pierden dicho carácter con la nueva edición que se publique, mientras que para el caso de datos obtenidos telemáticamente de una fuente accesible al público en formato electrónico, se establece que dicho carácter se pierda al transcurrir un año desde su obtención.

Por lo que respecta a las guías telefónicas, la LOPD considera que, en los términos previstos por su normativa específica, son fuentes accesibles al público siendo de aplicación las previsiones generales del artículo 28.3, al no existir precepto específico al respecto en la normativa sectorial.

Hechas estas consideraciones, y respecto del caso que nos ocupa, la empresa de marketing directo sancionada disponía de dos ficheros con datos obtenidos de las guías telefónicas, uno actualizado al año 2000 y otro al año 2001. Por error, la empresa utilizó el fichero más antiguo en una campaña que le encargó una empresa cliente, dándose la circunstancia de que la persona denunciante figuraba en dicho fichero y no en el correspondiente al año 2001, por haber sido excluido de dicho repertorio de abonados.

En la resolución, la Agencia consideró que la empresa de marketing había utilizado datos que, si bien en su día procedían de fuentes accesibles al público, habían perdido tal carácter en el momento en que se realizó la campaña objeto de la denuncia, por lo que para su utilización se hacía necesario disponer del consentimiento del afectado. Dado que no existía tal consentimiento, se sancionó a la empresa por una infracción de carácter grave.

La empresa sancionada alegó en su defensa que la utilización del fichero antiguo tuvo su origen en el error humano de un empleado que no utilizó la última versión del mismo. Frente a ello, la Agencia consideró que dicha alegación no exoneraba de responsabilidad a la empresa en el tratamiento de los datos personales del denunciante, por cuanto los datos personales contenidos en la versión antigua del fichero, de acuerdo con el artículo 16 de la LOPD, deberían haber sido bloqueados, 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. En la tramitación de las actuaciones se constató que la empresa sancionada no había procedido al bloqueo del fichero con la versión antigua.

4.1.3. *Campañas publicitarias de los operadores*

Otro conjunto lo forman dos resoluciones que han surgido como consecuencia de campañas publicitarias realizadas por empresas de telecomunicaciones, resultando éstas sancionadas.

La primera resolución tiene su origen en la remisión por parte de un operador móvil de mensajes SMS publicitarios, pese a que el cliente receptor de dichos mensajes había solicitado previamente al operador que cesara en la realización de dichos envíos. Este hecho fue considerado por la Agencia como una infracción del artículo 6.1 de la LOPD en relación con el artículo 68 del Real Decreto 1736/1998, de 31 de julio, siendo considerado como falta grave.

Alega la operadora en su descargo que dicha situación se produjo como consecuencia de no disponer de tecnología suficiente para evitar la comunicación publicitaria en una campaña masiva *«que se estaba fraguando con anterioridad al ejercicio del derecho de oposición»* y, como consecuencia de ello, estima que no ha existido dolo ni culpa por su parte.

Adicionalmente señala que la infracción imputada exige una conducta activa contraria a las instrucciones del cliente.

Sin embargo, las alegaciones de la operadora se limitaron a la mera declaración genérica de que carecían de la tecnología necesaria para evitar la comunicación, sin aportación de elemento probatorio que la sustente. En ningún momento la imputada había solicitado la practica de pruebas o había aportado información que permitiera acreditar fácticamente las dificultades técnicas alegadas, por lo que, dado el lapso temporal transcurrido entre la oposición del cliente y el envío de la comunicación no pueden ser apreciadas para excluir la culpabilidad. Y tampoco ha aportado información alguna sobre la conducta activa de la operadora realizadas para evitar que se produjera la comunicación comercial no deseada (por ejemplo comunicaciones a los responsables de la campaña para excluir al denunciante, dificultades derivadas de esa comunicación o cualquier otra que permitiera apreciar una actitud diligente por su parte). Limitándose a una mera manifestación genérica por lo que fue rechazada la alegación.

Por ello, la resolución declara que la operadora con su conducta consistente en enviar un mensaje telefónico al denunciante una vez comunicado su deseo de no recibirlos, trató los datos del reclamante sin su consentimiento, siendo tal conducta tipificada como infracción grave e imponiéndose la sanción en su grado mínimo y sin que, por tanto, fuese factible tipificarla de infracción leve como solicitó la operadora, pues vulneró la prohibición de enviarle mensajes telefónicos no por motivos formales, sino de fondo de la operativa de la empresa, transgrediéndose, uno de los principios fundamentales de la protección de datos como es la obtención previa del consentimiento cuando no se está excluido de obtenerlo.

La segunda resolución surge como consecuencia de una campaña publicitaria que un operador de telefonía móvil encargó a una empresa de marketing con objeto de hacer una oferta a los estudiantes y profesores de una universidad, encargándose la empresa de marketing de la obtención de los datos de los destinatarios, respecto de los cuales no se obtuvo el necesario consentimiento.

En la resolución de este caso se consideró al operador de telefonía móvil responsable del tratamiento realizado por la empresa de marketing, ya que fue dicho operador, en definitiva, el que decidió sobre la finalidad, contenido y uso de la campaña publicitaria, siendo sancionado por ello según señala la resolución, con independencia de los contratos privados que hubieran suscrito el operador y la empresa de marketing que pudieran determinar la posibilidad de repetir judicialmente contra esta última.

Finalmente, también se atribuyó una responsabilidad directa, y su correspondiente sanción, a la empresa de marketing por tratar unos datos sin conocer si existía consentimiento inequívoco de los interesados, ya que ésta no pudo acreditar el procedimiento mediante el cual obtuvo los datos.

4.1.4. *Cesión de datos a terceros*

La Agencia dictó una resolución como consecuencia de un procedimiento sancionador abierto a un operador de telecomunicaciones y a una plataforma de televisión de pago, existiendo entre ambas empresas un acuerdo por el cual la plataforma de televisión se convertía en agente para la venta y comercialización de diversos productos de telecomunicación facilitados por el operador: servicio de telefonía fija en acceso indirecto y bonos para el acceso telefónico a Internet.

En base al acuerdo anterior, la plataforma de televisión comunicó datos de clientes al operador de telecomunicaciones cuando el cliente solicitó a la plataforma de televisión disponer de acceso a Internet, ya que dicho servicio era realmente proporcionado por el operador de telecomunicaciones. Este último emitió, al cabo del tiempo, facturas a nombre del cliente de la plataforma de televisión por servicios de telefonía fija en acceso indirecto, lo que provocó la denuncia del cliente.

Si bien ambas empresas alegaron que dicha comunicación quedaba amparada en el artículo 12 de la LOPD por tratarse de una prestación de servicios existente entre ambas empresas en base al contrato de agencia ya citado, la Agencia consideró que la citada comunicación quedaba encuadrada en el marco del artículo 11 de la LOPD con base en dos motivos: la ausencia de información al cliente y el hecho de que éste celebrara únicamente un contrato con la plataforma de televisión.

La circunstancia anterior, unida a la inexistencia de un consentimiento inequívoco por parte del cliente para la cesión de sus datos, motivó que se sancionara a la plataforma de televisión por una infracción del artículo 11 calificada como muy grave.

4.1.5. *Otros*

Finalmente, cabe hacer referencia a una resolución dictada como consecuencia de una inspección realizada de oficio a un operador de telefonía móvil que concluyó con la imposición de cuatro sanciones por otras tantas infracciones que a continuación se resumen:

- La primera de ellas surge como consecuencia del hecho de que los usuarios del departamento de marketing de la citada empresa disponían de acceso, para la realización de su actividad, a los datos de tráfico y facturación relativos a sus clientes, sin que el operador haya podido acreditar disponer del consentimiento para el tratamiento de dichos datos con fines de marketing. Lo anterior, fue considerado por la Agencia una infracción del artículo 6 de la LOPD en relación con el artículo 65.3 del Real Decreto 1736/1998, de 31 de julio, que traspone la Directiva CE/97/66, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el

sector de las telecomunicaciones. Según esta normativa sectorial, el tratamiento en cuestión requiere un consentimiento específico del que carecía el operador.

- La segunda de las infracciones resulta del hecho de que el citado operador comunicaba periódicamente a dos empresas de informes comerciales los datos bancarios que figuraban en el contrato de sus nuevos clientes, con el fin de que estas empresas confirmaran con el banco del cliente si los datos facilitados por éste eran correctos. Realizada dicha gestión, ambas empresas devolvían al operador un fichero informático con más datos de los que se le encargó comprobar, entre los que se encontraba la siguiente información acerca de la cuenta del cliente: si disponía de tarjeta de crédito y de recibos domiciliados, el saldo medio de la cuenta y si percibía pensión o nómina, datos que fueron incorporados por el operador a su propio sistema informático.

  La Agencia entendió, inicialmente, que existía una responsabilidad por parte del operador a la hora de acreditar el consentimiento para el tratamiento de tales datos, a lo que el operador alegó que correspondía a las empresas con las que tenía contratada la prestación de servicios recabar el consentimiento de los afectados, debiendo de recaer sobre éstas últimas la responsabilidad en caso de no recabarse. Finalmente la Agencia, citando sentencias de la Audiencia Nacional, resolvió sancionar al operador por considerar que, si bien no puede serle exigido al cesionario la obtención del previo consentimiento de los datos cedidos, pues dicha obligación es del cedente, tal y como alegaba el operador, sí es carga del cesionario aportar la documentación que justifique que, al menos y conforme a parámetros de razonable diligencia, éste había verificado la existencia de dicho consentimiento.

  Al no justificar el operador lo anteriormente expuesto fue sancionado por una infracción del artículo 6 de la LOPD calificada como falta grave.

- La tercera infracción se produce al comprobar que el operador incorporaba y mantenía en su sistema informático datos extraídos de las consultas efectuadas en su día sobre sus clientes en ficheros de morosidad comunes regulados en el artículo 29 de la LOPD, tales como importe de la deuda, entidad informante, número de impagados, sin que tales datos fuesen posteriormente actualizados. Este hecho fue sancionado como infracción del artículo 4.3 de la LOPD, al considerar la Agencia que, de acuerdo con el artículo 4 de la LOPD, únicamente pueden someterse a tratamiento aquellos datos que, siendo adecuados, pertinentes y no excesivos, supongan la existencia de una información exacta y que se encuentre puesta al día de forma que responda con veracidad a la situación actual del afectado.

  Frente a esta postura el operador alegó, en el recurso de reposición interpuesto contra la resolución, que no se dedica al suministro de información sobre solvencia y que tales

datos no inducen a error sobre el estado actual de la solvencia de sus clientes ya que dichos datos, junto con otros datos del cliente, se unen indisolublemente a una fecha, sin que el operador tome decisiones frente a los clientes basadas en datos no actualizados. Añadió, además, que los clientes prestan su consentimiento para que se compruebe su solvencia a través de las condiciones generales de contratación, exponiendo también la dificultad de mantener actualizados los datos sin la colaboración de las entidades de información sobre solvencia, así como del borrado selectivo de dichos datos.

Las argumentaciones del operador fueron acogidas por la Agencia, toda vez que el operador mantiene en sus ficheros el resultado de la consulta que en su día efectuó al fichero de morosidad para evaluar el nivel de riesgo de las personas que contrataron con ella la prestación del servicio de telefonía. Por ello, y dado que son datos asociados a sus clientes, que se conservan junto con otros datos del cliente para el mantenimiento de la relación contractual, cabe entender que el operador puede conservar en sus ficheros los datos obtenidos de la consulta al fichero de morosidad en el momento de la firma del contrato, pues no son utilizados por el operador para otra finalidad distinta de aquella para la cual los clientes prestaron su consentimiento, esto es, para la comprobación de su solvencia económica en el marco de la relación contractual, manteniéndose asociados a los demás datos del cliente.

En base a lo anterior, la Agencia revocó la resolución dictada y, en consecuencia, la sanción impuesta previamente.

- Finalmente, la cuarta infracción tiene su origen en una deficiencia detectada en el contrato de adhesión de sus clientes en relación con las condiciones generales contenidas en el mismo. En las citadas condiciones generales se establecía que los datos personales que se recaban en un apartado concreto del contrato tienen el carácter de opcionales, informándose de las consecuencias que se aplicarían en caso de que dichos datos no fuesen aportados. La deficiencia radicaba en que el apartado concreto de datos opcionales que se indicaba en las condiciones generales no tenía correspondencia alguna en el contrato. Esta situación, que ya había sido detectada anteriormente y que motivó en su día que el Director de la Agencia instara al citado operador para que la subsanara, seguía persistiendo, siendo este hecho constitutivo de una infracción del artículo 5.1 de la LOPD.

4.2. Sanidad

La mayor parte de las denuncias presentadas ante la Agencia en relación con tratamientos de datos relativos a la salud, se refieren a comunicación de datos y al tratamiento de los mismos sin consentimiento expreso de los afectados. Se detallan a continuación las Resoluciones más importantes.

Comunicación de datos existentes en un Banco de Sangre

En la Memoria relativa al año 2001 se informó de una denuncia sobre la cual no se había dictado resolución, en relación con 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.

Al finalizar el año 2001 se encontraba en tramitación el procedimiento sancionador iniciado al Banco de Sangre y a la Hermandad de Donantes de Sangre por cesión de datos de salud entre ambas entidades, en el que la Hermandad de Donantes no pudo acreditar que tratase los datos del denunciante con consentimiento expreso del afectado, y el Banco de Sangre no pudo acreditar que contase con el consentimiento previo del denunciante para ceder sus datos a la Hermandad de Donantes.

La Resolución del procedimiento declaró que el tratamiento de datos del denunciante realizado por la Hermandad de Donantes y la cesión de los mismos por parte del Banco de Sangre quedaban al margen de los supuestos permitidos en los artículos 6, 7 y 11 de la LOPD, resolviendo el Director imponer al Banco de Sangre una multa de 60.101,21 euros por una infracción del artículo 11.1 de la citada norma, tipificada como muy grave, e imponer a la Hermandad de Donantes de Sangre una multa de 60.101,21 por una infracción del artículo 7.3 de la misma, tipificada como muy grave en el artículo 44.4.c) de dicha norma.

Comunicación de datos de un gabinete médico a una compañía de seguros

En la Memoria relativa al año 2001 también se informó de una denuncia sobre la cual aún no se había dictado resolución, en la que 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 médicos relativos a sus estados de salud. Estos informes fueron presentados por la empresa de seguros en los autos del Juicio Verbal pertinente que se seguían en un Juzgado de Primera Instancia, sin que ellas dieran su consentimiento para la utilización, tratamiento y difusión de tales datos.

Tras la realización de actuaciones inspectoras, se determinó que el Gabinete de Médicos realizaba una prestación de servicios para la empresa de seguros. Sin embargo no se habían cumplido los requisitos especificados en el artículo 12 de la LOPD, motivo por el cual el Director de la Agencia acordó el inicio de un procedimiento sancionador al Gabinete Médico por infracción del artículo 11 de la LOPD, que se resolvió imponiendo al Gabinete Médico una multa

de 60.101,21 euros por haber comunicado los datos de salud de las afectadas a la compañía de seguros, sin que existiera, cuando se produjeron los hechos, un contrato para la prestación de servicios entre ambas entidades.

4.3. Publicidad y Prospección Comercial

A lo largo de 2002 se han dictado 19 resoluciones sancionadoras relativas a tratamientos realizados con fines de publicidad y de prospección comercial, lo que supone aproximadamente un 20% del total de resoluciones relativas a ficheros de titularidad privada.

Si bien tres de las sanciones impuestas lo han sido por la obstaculización del derecho de acceso de los destinatarios de distintos envíos publicitarios, en general la infracción más sancionada es la tipificada en el artículo 44.3.d de la Ley Orgánica, consistente en tratar datos de carácter personal que no proceden de fuentes accesibles al público, que no han sido facilitados por los propios interesados o que no han sido obtenidos con el consentimiento de éstos. Así, se ha sancionado el envío postal de publicidad por parte de empresas privadas a personas que no han prestado su consentimiento y cuyos datos proceden, respectivamente, del Censo Electoral (en tres casos), de los ficheros de personal de una Diputación Provincial y de dos universidades públicas. También se ha sancionado a unos grandes almacenes por tratar con idéntica finalidad los datos de un cliente que previamente había solicitado su cancelación.

Así mismo, se sancionó en dos ocasiones el incumplimiento de la obligación prevista en el artículo 26 de la Ley Orgánica, sobre notificación e inscripción de ficheros, en este caso de datos de carácter personal destinados a la prospección comercial y que, en uno de los casos, se habían recabado inicialmente para desarrollar una actividad de representación artística de menores de edad.

En relación con el régimen normativo que configura el artículo 28 de la Ley Orgánica, respecto de los datos incluidos en las fuentes de acceso público, ha sido sancionada una compañía especializada del sector que nos ocupa, por el tratamiento con fines publicitarios de datos contenidos en una versión no actualizada de los repertorios telefónicos, que habían perdido su carácter de fuente accesible al público tras la nueva edición publicada, de conformidad con lo que establece el apartado 3 del mencionado artículo.

Por otra parte, deben destacarse por su relevancia las sanciones impuestas a distintas compañías de un grupo empresarial del sector energético por la utilización con fines comerciales de los datos de clientes de las empresas suministradoras por parte de las otras compañías, teniendo como base las denuncias presentadas por varios de esos clientes. Las empresas suministradoras habían enviado una carta a sus clientes en el mes de diciembre de 1999, informándoles de la especialización de sus actividades y del incremento del número de empresas

del grupo. Pedían el consentimiento a los clientes para recibir información de sus ofertas y, en el caso de no dar ese consentimiento, debían rellenar un folleto que se adjuntaba o llamar a un número de teléfono gratuito. Para hacer llegar esta carta a cada una de las personas afectadas contrataron con una tercera empresa, que se encargaría de introducir la carta en los buzones de los clientes. La solicitud de consentimiento tácito era válida, pero las empresas solicitantes debían acreditar que cada cliente había recibido la carta de solicitud.

Respecto de la primera de las denuncias que ocasionó el inicio del procedimiento sancionador, en aplicación del principio constitucional de *«presunción de inocencia»* y del principio «*in dubio pro reo*», no pudo imputarse la cesión de los datos sin consentimiento, puesto que el propio denunciante había declarado que no podía asegurar si recibió o no la mencionada carta. En otro de los casos, la empresa que distribuyó las cartas certificó que le constaba que la carta del denunciante se había distribuido sin incidencias en su entrega, por lo que, aunque podrían plantearse dudas sobre si se había obtenido el consentimiento tácito, tampoco cupo declarar que la suministradora hubiera incurrido en infracción de la LOPD.

Diferente era la situación de la otra suministradora de gas, respecto de la cual se habían recibido dos denuncias. En ambos casos se aportó una certificación sobre la entrega de las respectivas cartas. Sin embargo, este certificado no había sido elaborado con el rigor que requiere el contenido de lo certificado, dado que la entidad certificadora no era la misma que había preparado, impreso y distribuido las cartas.

Por consiguiente, la Resolución estimó que la segunda de las empresas suministradoras había cedido datos de algunos de sus clientes a otras empresas de su grupo empresarial sin haber obtenido previamente su consentimiento, al no poder acreditar la recepción de las cartas enviadas. Por otra parte, la compañía cesionaria estaba obligada a tratar los datos sólo tras verificar si las dos empresas cedentes habían obtenido el consentimiento de los interesados, de conformidad con lo señalado en el artículo 11.5 de la LOPD, por lo que, al no haberse asegurado de ello, se resolvió que también había incurrido en infracción.

Finalmente, resulta interesante mencionar las sanciones impuestas, respectivamente, a una editorial, una compañía especializada en acciones de venta a distancia y otra que organiza cursos por correspondencia. Durante la tramitación del procedimiento sancionador quedó acreditado que la primera había comunicado a las otras dos los datos del denunciante sin su consentimiento previo y sin que concurriese ninguna de las circunstancias que permiten prescindir del mismo, en los términos del artículo 11.2 de la Ley Orgánica. Tales datos habían sido posteriormente utilizados por las cesionarias para dirigir al afectado una comunicación comercial con el objetivo de captarle como nuevo cliente. Para ello, previamente éstas últimas habían encomendado a otras dos compañías la realización de un proceso de duplicación sobre el fichero cedido, con objeto de descartar de la acción publicitaria a todas aquellas personas que ya formaban parte de sus respectivos ficheros de clientes.

Así, aun cuando las cesionarias manifestaron no haber participado en el mencionado proceso, en la Resolución se argumentó, de acuerdo con el criterio mantenido por la Sala de lo Contencioso Administrativo de la Audiencia Nacional, en Sentencia de 21 de junio de 2002, que para que exista un responsable del fichero o del tratamiento de datos personales no es necesario que se produzca un acceso físico a la información. En este sentido, la citada sentencia señalaba que *«... la figura del responsable del fichero se conecta, pues, en la Ley, con el poder de decisión sobre la finalidad, contenido y uso del tratamiento, poder en la decisión que ha de diferenciarse de la realización material de actividades que integran el tratamiento, ya que será responsable tanto quien decida y trate como quien, teniendo poder de decisión, encomiende la materialidad del tratamiento a un tercero que actúe bajo la dependencia o instrucciones del primero...»*.

4.4. Servicios de Internet

A lo largo del año 2002 se han realizado numerosas actividades de inspección con relación a actividades desarrolladas en Internet. Asimismo, se han dictado diferentes resoluciones en las que los hechos objeto de consideración se han situado en ese mismo ámbito, de las que extraemos, por su relevancia, las que a continuación se reseñan.

Deber de secreto

En el año 2001 tuvo entrada en la Agencia de Protección de Datos una denuncia en la que se ponía de manifiesto que un sitio web, que ofrecía entre sus servicios la posibilidad de remitir *«postales»* a través del correo electrónico, permitía el acceso libre al contenido de las mismas así como a las direcciones de correo electrónico del remitente y del receptor.

En el desarrollo de las actuaciones previas de inspección se acreditó de forma fehaciente que durante un corto período habían quedado a disposición de cualquier usuario de ese sitio web todos los textos y direcciones de correo de aquellas personas que habían utilizado dicha opción, no mediando para dicho acceso ningún mecanismo de control previo.

De esta forma, y considerando el carácter de dato personal que alcanza a la dirección de correo electrónico cuando su estructura permite la vinculación directa o indirecta con una persona física, así como el hecho de que el tratamiento de datos personales en Internet debe respetar los principios de protección de datos, se consideró en la Resolución del procedimiento que se había vulnerado el deber de secreto respecto de los datos personales objeto de tratamiento, sancionándose como infracción leve, de acuerdo a lo establecido en el artículo 44.2.e de la Ley Orgánica 15/1999.

Otro caso en el que concurren similares circunstancias tuvo lugar en una entidad que, como parte del conjunto de servicios ofrecidos a sus clientes, mantenía una lista de distribución de correo electrónico a través de la cual remitía diversas comunicaciones a todos los usuarios.

Como resultado de un error en la configuración del sistema de envíos, las respuestas y consultas de clientes que en origen se remitían a una dirección de correo electrónico, asignada al Administrador del Sistema, fueron reenviadas durante un corto período de tiempo al conjunto de los usuarios del servicio, incluyendo los textos y las direcciones de correo electrónico asociadas.

En este caso se alegó, por parte de la entidad imputada, la involuntariedad en el hecho que causó el error del sistema que está en el origen de los envíos, la pronta corrección del mismo una vez detectado y la ausencia de perjuicio para los afectados. Además, se cuestionaba en dichas alegaciones el carácter de dato personal de la dirección de correo electrónico. La resolución del procedimiento, rebate la consideración de la falta de culpabilidad como eximente de sanción alegada por la entidad, con el argumento de que si bien ese tipo de conductas no tienen *«per se»* un carácter doloso, y en la mayoría de los casos presentan una falta de intencionalidad, basta con la simple negligencia en el cumplimiento de los deberes impuestos por la Ley a los responsables de los ficheros para que estas conductas puedan ser objeto de sanción conforme a lo establecido en la LOPD.

Derecho de oposición a la transferencia de datos de carácter personal

En abril de 2002 se recibió una denuncia en la que se ponían en conocimiento de la Agencia de Protección de Datos hechos relacionados con la comunicación, a través del correo electrónico, de la transferencia de los datos personales de los usuarios de un servicio ofrecido por una entidad a través de su sitio web a otra empresa, nueva titular de dicho servicio, en la que se manifestaba la posibilidad de oponerse a dicho acto a través de comunicación en ese sentido remitida por correo ordinario. Entendían los denunciantes que, al limitar las entidades responsables la forma en la que se podía ejercer ese derecho, se limitaba el ejercicio eficaz del mismo.

En el desarrollo de las actuaciones de inspección se acreditó que se había procedido a informar al Registro General de Protección de Datos sobre el cambio de titularidad del fichero así como que dicho cambio se había producido en el marco de un contrato de liquidación, cesión de crédito y compraventa firmado entre ambas entidades.

En cuanto a la comunicación realizada a los usuarios del servicio, se comprobó que en la misma se notificaba la comunicación de los datos personales de los usuarios a la entidad adquirente, indicando las finalidades con las que iban a ser tratados los mismos y solici-

tando de forma tácita el consentimiento inequívoco tanto para la cesión de los datos a la nueva entidad responsable, como para el tratamiento y cesión de esos mismos datos por parte de la empresa cesionaria, incluyendo la posibilidad de «*ceder y comunicar sus datos personales a otras entidades interesadas en proporcionar información comercial».* Finalizaba la comunicación ofreciendo un plazo para comunicar a la entidad cedente la oposición del usuario a dicha cesión mediante la remisión de un escrito a la dirección postal que se reseñaba y comunicando el sistema para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición arbitrado por la nueva entidad responsable.

Finalizadas las actuaciones de inspección, se acordó, por parte del Director de la Agencia de Protección de Datos el archivo de las actuaciones realizadas, mediante resolución en la que se hacía referencia a la licitud del procedimiento utilizado para recabar el consentimiento tácito, al encontrarse admitido tanto con carácter general —artículo 1253 del Código Civil— como por lo establecido en la Ley Orgánica 15/1999, con las excepciones en las que esta última exige, por la naturaleza de los datos cedidos, el consentimiento expreso de los interesados. Se señalaba también que, al informar de la finalidad de la cesión y de la actividad de la empresa cesionaria, se actuaba de conformidad con lo establecido en el artículo 11.3 del citado precepto.

No obstante lo anterior, se hacía constar que la pretensión de la comunicación remitida a los clientes del servicio dirigida a recabar el consentimiento para que la empresa cesionaria, nueva responsable del tratamiento, pudiera ceder sus datos a «*otras entidades pertenecientes al mismo grupo empresarial y/o otras empresas o entidades relacionadas o terceros interesados en proporcionarle a usted información comercial respecto a productos y/o servicios que puedan ser de su interés»,* no resultaba suficiente para satisfacer el principio de finalidad, al no permitir conocer el tipo de actividad a la que se dedica aquél a quién se pretende comunicar los datos. Por ello, señalaba la citada resolución, las cesiones que se efectúen al amparo de dicha cláusula no serán ajustadas a la Ley Orgánica 15/1999 por no cumplir con las exigencias contenidas en el apartado 3 del artículo 11 de dicha norma.

Transferencia Internacional de Datos

Durante el año 2002 se resolvió también el procedimiento sancionador iniciado a una compañía prestadora de servicios en Internet, como consecuencia de la denuncia presentada por un ciudadano con relación a un escrito del ayuntamiento de su municipio de residencia en el que se le ofrecía a él y a sus familiares la posibilidad de tener una cuenta de correo electrónico, dándoles a elegir entre una serie de opciones, de las cuales una era el nombre y primer apellido. Solicitada información al ayuntamiento responsable, éste contesto en el sentido de manifestar que se trataba de un proyecto de la corporación municipal concebido para potenciar el uso de las nuevas tecnologías de la información por parte de particu-

lares, industria, comercio y la propia administración, siendo una de las acciones consideradas el implantar un servicio de correo electrónico para particulares y empresas radicadas en el municipio, con carácter gratuito.

A tales efectos se había contratado la creación de un sitio web —un portal— a una empresa, a la que se cedió un fichero automatizado creado por el personal del ayuntamiento a partir de los datos del Padrón Municipal de Habitantes, integrado por un conjunto de registros cuya estructura incluía un código de usuario, una contraseña y una dirección de correo electrónico. Asimismo, como se pudo comprobar en el desarrollo de la actividad inspectora, ese fichero fue utilizado para dar de alta diversas cuentas de usuario en un servidor de correo electrónico cuya titularidad correspondía a una empresa radicada en los Estados Unidos de América, con la que la entidad española mantenía un contrato de hospedaje (*hosting)* de servicios.

A la vista del resultado de las actuaciones previas realizadas, se acordó, por parte del Director de la Agencia de Protección de Datos, el inicio de un procedimiento sancionador a la empresa contratada por el Ayuntamiento por presunta infracción de los artículos 6 y 33 de la Ley Orgánica 15/1999.

Respecto de la posible infracción del artículo 33, relacionada con la transferencia internacional de datos, la entidad basó sus alegaciones en el hecho de que el servidor donde se hospedaba el servicio de correo electrónico del ayuntamiento con el que había contratado se encontrase físicamente en los Estados Unidos de América no implicaba que hubiera acceso a los datos en él almacenados desde aquel país, ya que el contrato suscrito entre ambas entidades para el servicio de hospedaje establecía de forma expresa que la entidad encargada del alojamiento de los datos no podría, bajo ninguna circunstancia, acceder a información privada o a ficheros personales de ninguna clase, en los sistemas donde se trataran los datos objeto de custodia.

En una comunicación posterior, la entidad objeto del procedimiento sancionador aportó el contrato de servicios firmado con el ayuntamiento, cuya fecha de efectos era posterior a aquella en la que tuvieron lugar los hechos denunciados, y en el que no se reflejaba el hecho de que el hospedaje de los datos se realizaba en sistemas radicados en Estados Unidos de América. Asimismo, en el momento en el que el usuario aceptaba como suya una de las direcciones de correo electrónico propuestas al hacer uso del servicio por primera vez, no se le informaba de que dicho servicio radicaba en los Estados Unidos de América, no existiendo, por tanto, consentimiento para dicha transferencia de datos.

Por otro lado, había quedado acreditado que el ayuntamiento había facilitado a la empresa responsable del servicio un fichero automatizado con datos de carácter personal sin haber pedido de forma previa el consentimiento a los vecinos, con lo que ésta última entidad trató los datos de los habitantes del municipio sin contar con su consentimiento. En este sentido,

se alegó por parte de la empresa que el hecho de que el encargo viniera de una Administración otorgaba apariencia de legitimidad a la posesión de los datos que les habían facilitado, indicando además que las cuentas de correo no estaban vinculadas a su potencial titular de forma directa, ya que cuando fueron configuradas constituían una mera opción que el usuario debía decidir de forma expresa si aceptaba o no como dirección de correo electrónico. Por tanto, se consideraba por parte de la entidad responsable del servicio que su tratamiento estaba amparado por lo establecido por el artículo 12 de la Ley Orgánica 15/1999.

La resolución hace un detallado análisis centrado en el hecho de que de la lectura del artículo 12 de la Ley Orgánica 15/1999 se deduce que, para que concurra la figura de *«acceso a los datos por cuenta de tercero»,* la relación debe estar regulada en un contrato que debe constar por escrito o en alguna forma que permita acreditar su celebración y contenido. De esta manera se impone un requisito formal por cuanto que el contrato o bien debe constar en forma fehaciente o, en todo caso, ha de existir acreditación formal de su celebración. La Ley impone que siempre exista una relación jurídica de naturaleza contractual entre el responsable y el tercero al que encarga el tratamiento y, además, demanda una constancia formal de la misma, exigencia que es congruente con el sistema de protección establecido en la norma ya que, sin consentimiento ni conocimiento de los afectados se está permitiendo un tratamiento de sus datos personales por parte de un tercero.

Por ello, es preciso que conste quién es el responsable de dicho tratamiento y que éste se encuentre vinculado jurídicamente con el tercero para poder exigirle, en virtud de dicha relación jurídica, el cumplimiento de las garantías legales previstas. Item más, deviene exigible que figure detallado de forma explícita el conjunto de instrucciones del responsable del fichero al tercero responsable del tratamiento a realizar, de forma que este último sólo estará habilitado para tratar los datos conforme a aquéllas, no pudiendo aplicarlos ni utilizarlos para fines distintos de los que expresamente se estipulen, ni, comunicarlos, ni siquiera para su conservación, a otras personas.

Dado que en la fecha en la que tuvieron lugar los hechos denunciados no existía contrato o documento análogo entre la entidad responsable del servicio y el ayuntamiento responsable de los datos, no se podía considerar que el servicio prestado tuviera encaje en lo establecido en el artículo 12 de la Ley Orgánica de Protección de Datos.

Como consecuencia de todo lo anterior, el Director de la Agencia de Protección de Datos resolvió imponer a la entidad imputada sendas multas por la infracción de los artículos 6 y 33 de la Ley Orgánica 15/1999, si bien en el primer caso se aplicó la previsión del artículo 45.2 de la citada norma, al considerar que la responsabilidad de la empresa quedaba atenuada, en este supuesto concreto, por la confianza que la misma podía mantener en la conducta de la Administración. Las actuaciones relativas a la Corporación Municipal se incluyen en el apartado correspondiente de la memoria.

Medidas de seguridad en el acceso a ficheros automatizados con datos de carácter personal

Se produjo también el pasado año la resolución de una denuncia presentada ante Agencia de Protección de Datos en el año 2001 por una asociación, en la que se ponía en conocimiento de la misma el acceso, a través de Internet, a datos de carácter personal correspondientes a los usuarios de uno de los productos comercializados por una entidad proveedora de servicios de acceso a Internet a través de ADSL.

De las actuaciones previas realizadas por la Inspección de Datos se pudo concluir que, como consecuencia de una avería en el sistema informático en el que se ubicaba el fichero automatizado con la información relativa a las órdenes de instalación del servicio de acceso a Internet, combinada con un deficiente funcionamiento de los sistemas definidos para la realización de copias de respaldo y recuperación de datos, se tuvo que optar, por parte de la entidad responsable, por realizar un procedimiento de recuperación que tuvo como consecuencia la aparición de una vía alternativa de acceso a la información. Esta alternativa carecía de un control de acceso en las condiciones de seguridad establecidas de forma habitual. Como consecuencia de ello se produjeron accesos a datos personales de los clientes de servicio por parte de personas que no eran usuarios autorizados del sistema, accesos que no pudieron ser evitados por los mecanismos existentes.

En virtud de lo anterior, se decidió, por parte del Director de la Agencia de Protección de Datos, incoar procedimiento sancionador a la entidad responsable por infracción del artículo 9 de la Ley Orgánica 15/1999, en relación con lo establecido en el artículo 14 del Real Decreto 994/1999. La imputada, en sus alegaciones, manifestó que los accesos se produjeron motivados por una situación imprevisible y con una absoluta carencia de intencionalidad por su parte, señalando además que dichos hechos únicamente podían haber sido ejecutados tras una búsqueda de puntos débiles en sus sistemas de seguridad que en ningún momento podían tener un objetivo lícito. Reforzaba su argumentación haciendo constar que los responsables de los accesos en ningún momento se habían puesto en contacto con ellos para advertirles de dicha posibilidad, si bien aprovecharon el intervalo temporal en que fue posible para la descarga de ficheros cuya titularidad no les correspondía.

En cuanto a los procedimientos de copia de respaldo y restauración de datos, manifestaron que los datos correspondientes al servicio que sufrió la avería no eran objeto de copia por el enorme esfuerzo técnico que requería y porque la continuidad en las modificaciones y actualizaciones de los datos en el sistema responsable acarreaba un consumo de recursos innecesarios que redundaba en la falta de operatividad del mismo.

Frente a dichas alegaciones, en la resolución del procedimiento sancionador se hacían diversas precisiones al respecto basadas en lo establecido en el Reglamento de Medidas de

Seguridad. Dicha norma establece una serie de medidas que, en su conjunto, proporcionan un determinado nivel de seguridad, siendo determinante la idea del conjunto puesto que la presencia de debilidades en alguna de las medidas puede hacer inútiles las otras por muy robusta que sea su definición e implementación. De aquí que en la literatura especializada se considere el concepto de arquitectura de seguridad como referido a un conjunto integrado e interdependiente de reglas de servicio en contraposición al concepto de una serie de medidas aisladas e independientes entre sí.

En este sentido, y en lo que tiene que ver con los sistemas de información, la arquitectura de seguridad de un sistema de estas características se ha de sustentar en tres pilares definidos por los conceptos de confidencialidad, integridad y disponibilidad, pilares que, siguiendo con la idea anterior, lejos de estar aislados se complementan entre ellos con un elevado grado de sinergia, hasta tal punto que, en ocasiones, un fallo en uno de ellos provoca deficiencias en los restantes.

En el caso objeto de análisis el foco de atención se centró en lo prevenido en el artículo 14 con relación a las copias de respaldo y recuperación de datos (disponibilidad), y en el artículo 12, que establece las medidas a adoptar respecto al control de accesos (confidencialidad), ambos artículos del citado Reglamento de Medidas de Seguridad.

El artículo 14 constituye uno de los cimientos de la disponibilidad, al proveer a los sistemas de la capacidad de acceder a la información tras ocurrir un hecho que provoque una interrupción no deliberada en los accesos a la información, bien sea por causas naturales, bien por mal funcionamiento de los sistemas o por otras causas.

Esa capacidad de recuperación o reconstrucción de la información frente a una incidencia requiere, en primera instancia, de la disposición de una copia fiel de la información, es decir, del conjunto de los datos preexistentes al momento en que se produjo el fallo, tarea que es responsabilidad de los procedimientos de copia de respaldo que se hayan definido.

De igual forma, la eficacia de la reconstrucción requiere, además, de la capacidad de volver a disponer de la estructura que alberga dicha información así como de la de poder volver a reubicar los datos existentes, tarea que es asignada al procedimiento de recuperación de los datos.

Ambos procesos son interdependientes, necesitando el uno del otro, y ambos, en conjunción, son imprescindibles para que exista la capacidad de devolver al sistema al momento anterior al fallo con un grado adecuado de fiabilidad.

El artículo 14 obliga al responsable del fichero, y en su caso, al encargado del tratamiento, a avalar la disponibilidad de la información frente a la posibilidad de pérdida o

destrucción, mediante el concurso de la adecuada implementación de los procedimientos que han sido reseñados. En tal sentido establece el apartado segundo de dicho artículo la necesidad de garantizar la reconstrucción de forma que se retorne al momento anterior a la pérdida o fallo.

Además, fijado con claridad el objetivo y los medios para su consecución, el artículo 14 va aún más allá, ya que no solo establece la necesidad de la existencia de ambos procedimientos sino que obliga a la verificación de su correcta definición y funcionamiento. Es decir, se establece el mandato de comprobar que ambos procesos sean conformes a los objetivos establecidos y que cumplan su función en caso de que sea necesaria su aplicación.

Lo anterior implica en la práctica, de forma necesaria, como se recoge en la literatura especializada sobre seguridad, que los procedimientos sean definidos con un suficiente grado de detalle, requiriendo incluso de la realización de pruebas de los mismos una vez definidos y configurados. De esta forma, puede garantizarse la reconstrucción al verificar su adecuada definición y la correcta aplicación en el caso de que sea necesaria su uso.

Por último, el apartado tercero del artículo 14 determina un criterio de frecuencia que se ha de tener en cuenta a la hora de realizar las copias de respaldo, fijando una periodicidad mínima semanal, con la única salvedad de que en dicho intervalo no se haya producido ninguna actualización de los datos del fichero objeto de respaldo.

En cuanto al artículo 12, la resolución pone el acento en preservar los datos custodiados de accesos no autorizados, fijando, por un lado una limitación expresa del acceso de los usuarios autorizados del sistema a los datos que necesiten para el ejercicio de sus funciones y determinando, por otro, la obligación del responsable del fichero de establecer los mecanismos que garanticen el cumplimiento de dicha limitación.

Finalizado el razonamiento en los términos señalados, prosigue la resolución valorando los procedimientos establecidos por la entidad responsable del fichero automatizado respecto de las copias de respaldo, determinando la inexistencia de un procedimiento de copias de respaldo como tal y señalando que, frente al motivo aludido para no realizarlas, basado en el carácter dinámico de la información almacenada como resultado de su continua actualización, éste más bien debiera ser el argumento necesario para su realización, incluso con menor periodicidad a la establecida en el Reglamento de Seguridad.

En cuanto al procedimiento de recuperación, se reconoce la falta de detalle sobre las tareas a realizar, así como la ausencia de una adecuada descripción de las arquitecturas *hardware* y *software* necesarias para reconstruir el sistema. De esta forma, se con-

cluye en la resolución que hubo de improvisarse un procedimiento, hecho que determinó que se pusiera en marcha un sistema inestable que no debió haber entrado en producción.

En cuanto al argumento que presenta los accesos no autorizados como resultado de una manipulación técnica de búsqueda de debilidades del sistema, se considera que las debilidades presentes no hubieran tenido lugar si se hubieran adoptado las medidas de seguridad recogidas en los artículos 14 y 12 del Real Decreto 994/1999.

Como consecuencia, el Director de la Agencia de Protección de Datos resolvió imponer a la entidad imputada una sanción por infracción del artículo 9 de la Ley Orgánica 15/1999.

Control de accesos de usuarios de Banca Electrónica

En el año 2002 se resolvió también el procedimiento sancionador iniciado a una entidad financiera que ofrece servicios de Banca Electrónica, como consecuencia de la denuncia presentada por un usuario del citado servicio, en la que ponía de manifiesto que, en repetidas ocasiones, intentando acceder a través de Internet a su cuenta en dicha entidad financiera, tuvo acceso a los datos de otro cliente. Esta situación se produjo en repetidas conexiones, y empleando siempre sus propias claves. Como prueba de sus afirmaciones aportaba copias de pantalla en las que se visualizaban datos identificativos y financieros del otro cliente.

A lo largo de las actuaciones de inspección se determinó que efectivamente se habían producido dichos accesos como resultado de la conjunción de dos factores. Uno de ellos el hecho de que, como consecuencia de una caída en los sistemas de información manejados por los operadores telefónicos de la entidad, se asignara de forma manual el código de usuario del denunciante, resultado ser dicho código exactamente igual al del otro usuario preexistente. En cuanto al otro factor en liza, se determinó que al elegir ambos usuarios como clave de acceso al sistema su fecha de nacimiento, resultó que las mismas sólo diferían en dos caracteres, lo que posibilitaba, por mor del sistema de autorización de accesos implementado por la entidad, la realización de accesos no autorizados.

El procedimiento establecido por la entidad para la identificación de los usuarios a través de Internet en el momento en que se produjeron los hechos denunciados era el siguiente: Una vez situados en la página inicial del sitio web de la entidad el cliente debía identificarse (decir quien es) mediante la introducción del denominado código de usuario, para, de forma seguida, autenticarse (demostrar que es quien dice ser) mediante la introducción de dos posiciones aleatorias seleccionadas por el sistema de la clave de acceso.

Dado que el código de usuario era, debido a un error por la asignación manual, igual en ambos clientes, y que la clave de acceso presentaba una gran similitud, se infería que había una alta probabilidad de acceso por parte de ambos clientes a los datos del otro.

En cuanto a la valoración de los procedimientos establecidos por la entidad para la identificación de los clientes en los accesos al sistema, se señalaba que, bajo la hipótesis de una selección aleatoria de los códigos de usuario y claves de acceso de los clientes, el sistema utilizado proporcionaba suficientes elementos de seguridad, al utilizar un sistema de doble llave que hacía extremadamente baja la probabilidad de que un usuario pudiera entrar con las claves de otro.

Ahora bien, en la práctica, los procedimientos de asignación de claves y códigos habilitados sobre la tecnología producían una merma sustancial de los niveles de seguridad teóricos, ya que las claves y códigos no eran elegidos de forma aleatoria por el sistema, sino que eran determinados por el usuario en el proceso de alta, sin que se le informara a éste de la buena práctica de seleccionar claves que no fueran fácilmente predecibles a través de sus datos personales, por lo que tendía a seleccionar valores triviales o que se derivaban de forma directa de sus datos personales, con el detrimento sustancial que implicaba respecto de la seguridad teórica del sistema

Se ponía de manifiesto de esta forma que los controles establecidos por la entidad no habían resultado suficientes para garantizar la seguridad de los datos de sus clientes, concurriendo además el hecho de que, puesto que la información de un cliente que había sido accedida por otro distinto contenía datos identificativos, así como de movimientos y saldos de sus cuentas bancarias, se debía considerar dicha información como relativa a servicios financieros.

Dado que el apartado 2º del artículo 4 del Real Decreto 994/1999 establece que el responsable del fichero debe habilitar sobre los ficheros de servicios financieros las medidas de seguridad de nivel básico y de nivel medio recogidas en el citado Reglamento y que dentro del conjunto de medidas de ese último nivel se establece la obligación de utilizar un mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema, se concluye que se había producido una vulneración respecto de las medidas de seguridad que debía tener implantadas la entidad responsable tendentes a impedir el acceso de una persona a la cuenta de otra. Por consiguiente, no se había garantizado la identificación inequívoca y personalizada de los usuarios con acceso al sistema.

En consecuencia, en la Resolución se sancionó por infracción del artículo 9 de la Ley Orgánica 15/1999, en relación con el artículo 18 del Real Decreto 994/1999, que establece la obligación del responsable del fichero de 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.

4.5. Ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito

Durante el año 2002 los ficheros referidos a información sobre solvencia patrimonial y crédito, han originado un número ligeramente inferior de reclamaciones de tutela de derechos y de denuncias de posibles infracciones a la Ley Orgánica 15/1999 en relación con el año anterior.

De las Actuaciones de inspección iniciadas a lo largo del año 2002, aproximadamente un 18% de ellas hacían referencia a información contenida en ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito, en su mayoría relacionadas con entidades financieras y empresas de telecomunicaciones.

En cuanto a las tutelas de derecho, de las 447 iniciadas en el año 2002, aproximadamente el 20% estaban relacionadas con ficheros dedicados a la prestación de servicios de información sobre solvencia patrimonial y crédito.

Siguiendo la tendencia de años anteriores, durante el año 2002 del total de reclamaciones y denuncias recibidas relacionadas con este sector, el 97% hacen referencia a los cuatro ficheros de información sobre solvencia patrimonial y crédito más significativos

Durante el año 2002 se concluyeron 37 procedimientos sancionadores relacionados con este sector, de los que 9 fueron sobreseídos, imponiéndose en los 28 restantes sanciones a entidades encuadradas en dicho sector. Las principales infracciones fueron las siguientes:

a) En 30 casos la conculcación del principio de calidad de datos, establecido en el artículo 4 apartado 3 de la Ley Orgánica 15/1999.

b) En 3 casos la conculcación del principio de consentimiento del afectado en el tratamiento automatizado de sus datos personales, regulado por el artículo 6 de la misma norma.

c) En 3 casos la conculcación del derecho de rectificación y cancelación de datos personales, regulado por el artículo 16 de la Ley Orgánica 15/1999, que estipula que: *serán rectificados o cancelados, en su caso, los datos de carácter personal ... cuando resulten inexactos o incompletos.*

d) En 7 casos la conculcación de lo estipulado en el artículo 29 de la Ley Orgánica 15/1999, en lo referente al incumplimiento de los plazos de notificación de la inclusión en el fichero y al periodo de tiempo máximo en el que se pueden registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados.

e) En dos casos se ha aplicado con carácter excepcional el artículo 45.5 de la Ley Orgánica 15/1999.

La mayoría de los procedimientos incoados a entidades de solvencia patrimonial y crédito ha sido por incumplimiento del artículo 4.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que señala: «*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad de la situación actual del afectado».*

La obligación establecida en el artículo 4.3 trascrito impone la necesidad de que los datos personales que se recojan en cualquier fichero de datos sean exactos y respondan en todo momento a la situación actual de los afectados, siendo los responsables de los ficheros quienes responden del cumplimiento de esta obligación.

El incumplimiento de esta obligación está tipificado en el artículo 44.3.d) de la Ley Orgánica 15/1999 como infracción grave *(«Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave»)*.

En consecuencia, toda entidad, antes de incluir los datos de un afectado en un fichero común de solvencia patrimonial y crédito, debe proceder en la forma determinada en la Instrucción 1/1995, de 1 de marzo de 1995, de la Agencia de Protección de Datos que dispone que la inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias deberá efectuarse solamente cuando concurran los siguientes requisitos:

« Existencia previa de una deuda cierta vencida y exigible, que haya resultado impagada. Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación».

Entre las resoluciones dictadas en este ejercicio por infracción del artículo 4.3 de la Ley Orgánica 15/1999, cabe destacar los relacionados con la negligencia en que incurren ciertas entidades al realizar envíos de tarjetas de crédito a través de medios que imposibilitan tener certeza de su recepción, tal y como es el correo ordinario. Este hecho ha dado lugar a cargos de los que no se hace responsable el titular de la tarjeta. Ante el impago de dichos cargos, las entidades afectadas, a pesar de reconocer la pérdida de la tarjeta, han realizado inclusiones en ficheros comunes de solvencia.

De las alegaciones presentadas por una de dichas entidades ante esta Agencia durante la tramitación de un procedimiento sancionador, se dedujo que la misma había tenido cono-

cimiento de la pérdida de la tarjeta del afectado, por lo que no procedía informar con posterioridad al fichero común de solvencia la inclusión de la supuesta deuda con base en lo expresado en el artículo 4.3 de la citada Ley Orgánica 15/1999, al no haber acreditado dicha entidad que los datos correspondían con veracidad a la situación real del afectado.

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional 1144/1999, de fecha 16 de febrero de 2001 en el Fundamento de Derecho IV señala: *«Vista la conducta de la hoy actora, cabe apreciar que ha hecho uso de unos datos relativos a la insolvencia de una persona, conculcando los principios y garantías establecidas en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento de Datos de Carácter Personal, concretamente el de la certeza de los datos, que deben ser exactos, de forma que respondan con veracidad a la situación real del afectado, como exige su artículo 4.3.» En el mismo Fundamento de Derecho la sentencia continúa señalando que: «...ha de decirse que la inclusión equivocada o errónea de una persona en el registro de morosos, es un hecho de gran trascendencia de la que se pueden derivar consecuencias muy negativas para el afectado, en su vida profesional, comercial e incluso personal, que no es necesario detallar. En razón de ello, ha de extremarse la diligencia para que los posibles errores no se produzcan, cerciorándose previamente si la persona deudora es realmente aquella cuyos datos se facilitan a dicho registro».*

En algunos casos las entidades informantes, bien al contrastar inexactitud en las firmas de los comprobantes de compra, o bien al tener constancia de diversas irregularidades han procedido de inmediato a la cancelación de los datos de los afectados y a la denuncia de los hechos a la Policía, lo cual permitió apreciar una cualificada disminución de la culpabilidad y reducir la cuantía de la sanción en virtud del artículo 45.5 de la LOPD.

En relación con el incumplimiento de lo expresado en el artículo 29 de la Ley Orgánica 15/1999 cabe destacar el procedimiento incoado a una entidad financiera por haber comunicado datos personales de un cliente a un fichero común de solvencia patrimonial como consecuencia de un préstamo impagado, habiendo transcurrido más de seis años desde que la entidad, en cumplimiento de las cláusulas del contrato del préstamo, lo resolvió y dio por vencida la obligación.

Según la resolución, un préstamo es una obligación dineraria de cumplimiento periódico, en la que el prestatario se compromete a rembolsar tanto el capital como los intereses devengados. En el momento en que se produce la liquidación de la deuda por la entidad financiera deja de ser una obligación de cumplimiento periódico y pasa a tener una fecha de vencimiento de la obligación incumplida.

A este respecto, el artículo 29.4 de la Ley Orgánica 15/1999, de 13 de diciembre, establece que: *«sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuan-*

do sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos».

Por otro lado, la Instrucción 1/1995, de 1 de marzo, del Director de la Agencia de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito dispone en su norma tercera: *«El cómputo del plazo a que se refiere el artículo 28.2 de la Ley Orgánica (ahora 29.4) se iniciará a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso, desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico».*

En el presente caso, la fecha en que comienza a contar el plazo de seis años, es precisamente la de liquidación de la deuda que tuvo lugar cuatro años antes de la incorporación de los datos del afectado en el fichero de solvencia y no esta última fecha como pretendía el imputado.

Por lo expuesto, la entidad financiera incurrió en la conducta descrita en el artículo 44.3.f de la LOPD, que tipifica como infracción grave: *«Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara»*, ya que en el caso que nos ocupa, no se trataba de discutir la situación o no de deudor del afectado respecto de la entidad, sino de la posibilidad de incluir dichos datos en un fichero común de prestación de servicios de solvencia patrimonial y crédito transcurridos más de seis años desde la liquidación de la deuda.

Finalmente, debe destacarse un procedimiento iniciado en relación con la telecontratación de un servicio de telefonía de acceso indirecto, a través de una llamada al Centro de Atención al Cliente del operador, sin que exista documento acreditativo alguno. Para hacer efectiva dicha contratación, fueron recabados los datos de nombre, apellidos, domicilio y NIF del solicitante, así como el número de cuenta bancaria donde domiciliar las facturas y los números de teléfono en los que activar el servicio que se contrata.

La utilización de dichos servicios generó unas facturas que fueron devueltas por la entidad bancaria, figurando como motivo de la devolución *«Número de cuenta incorrecto»*. Asimismo se comprobó que el titular del servicio contratado no coincidía con el titular de las líneas telefónicas utilizadas como soporte.

A consecuencia del impago de las facturas, se incluyó una incidencia a nombre del titular del servicio en un fichero común de solvencia patrimonial.

Para que el tratamiento de los datos del afectado por parte del operador de telefonía hubiera resultado conforme con los preceptos de la L.O. 15/1999, hubieran debido concurrir en

el procedimiento examinado alguno de los supuestos contemplados en el artículo 6 de la Ley mencionada. Sin embargo, según declaró el interesado ante esta Agencia, él no había sido cliente de la citada entidad.

La entidad por su parte manifestó que, la contratación de sus servicios efectuada por teléfono por una persona justificaría el tratamiento de los datos de carácter personal para la efectividad de la relación negocial que se iniciaba en ese momento.

Efectivamente el sistema de contratación por teléfono es un método válido y admitido en derecho, regulado por el Real Decreto 1906/1999, de 17 de diciembre, que desarrolla el artículo 5.3 de la Ley 7/1998, de 13 de abril sobre condiciones generales de contratación.

El artículo 5.3 de la Ley 7/1998 establece: *«En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma».* El desarrollo reglamentario de este artículo se realiza a través del Real Decreto 1906/1999, de 17 de diciembre, en el que se ratifica la obligación de confirmación documental de la contratación efectuada por vía telefónica, electrónica o telemática.

Así, el artículo 5 del citado Real Decreto respecto a la atribución de la carga de la prueba dispone:

« La carga de la prueba sobre la existencia y contenido de la información previa de las cláusulas del contrato; de la entrega de las condiciones generales; de la justificación documental de la contratación una vez efectuada; de la renuncia expresa al derecho de resolución; así como de la correspondencia entre la información, entrega y justificación documental y al momento de sus respectivos envíos, corresponde al predisponente.
A estos efectos, y sin perjuicio de cualquier otro medio de prueba admitido en derecho, cualquier documento que contenga la citada información aun cuando no se haya extendido en soporte papel, como las cintas de grabaciones sonoras, los disquetes y, en particular, los documentos electrónicos y telemáticos, siempre que quede garantizada su autenticidad, la identificación fiable de los manifestantes, su integridad, la no alteración del contenido de lo manifestado, así como el momento de su emisión y recepción, será aceptada en su caso, como medio de prueba en los términos resultantes de la legislación aplicable...»

En el presente caso la entidad imputada no había acreditado que hubiera ratificado documentalmente la contratación efectuada. Este hecho unido a las evidencias de fraude en la contratación apreciadas posteriormente —el afectado no era titular de las líneas de teléfono contratadas ni de la cuenta bancaria declarada— permiten exigir una conducta diligen-

te antes de facilitar información de carácter personal a terceros. Ordenar la inclusión de datos de carácter personal en un fichero que presta información sobre el cumplimiento e incumplimiento de obligaciones dinerarias exige que se extreme la diligencia debida cuando existen dudas de la veracidad de los datos a comunicar.

A este respecto la resolución cita jurisprudencia del Tribunal Supremo (STS 16/04/91 y STS 22/04/91) que considera que del elemento culpabilista se desprende *«que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable.» El mismo Tribunal razona que «no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa» sino que es preciso «que se ha empleado la diligencia que era exigible por quien aduce su inexistencia.»* (STS 23/01/98).

A mayor abundamiento, la Audiencia Nacional por Sentencia de 29 de junio de 2001, en materia de protección de datos de carácter personal, ha declarado *que «basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia...».*

4.6. Entidades Financieras

Durante el año 2002 se han iniciado 77 actuaciones de investigación al objeto de esclarecer las denuncias presentadas por los ciudadanos contra las entidades financieras, sin contabilizar las relacionadas con ficheros a los que se refiere el artículo 29 de la LOPD, lo que supone un incremento de un 50% con respecto a las reclamaciones interpuestas durante el año 2001. Así mismo, se han atendido 34 reclamaciones de tutela de los derechos de acceso, rectificación, cancelación y oposición ejercidos por los ciudadanos ante estas entidades sin obtener resultados satisfactorios.

De las 77 actuaciones previas de investigación iniciadas, 33 concluyeron con el archivo de las actuaciones y 13 dieron lugar a la apertura de un procedimiento sancionador, continuando el resto en fase de investigación al finalizar el año.

El 80% de los procedimientos sancionadores finalizados durante el año 2002 se han resuelto con la imposición de sanciones siendo los hechos mayoritariamente sancionados por la infracción de los artículos 4.2 y 4.3 (calidad de datos) de la LOPD, seguido del artículo 10 (deber de secreto) y el artículo 6 (consentimiento del afectado). También han sido sancionadas, aunque con menor frecuencia, las infracciones a los artículos 18 (Tutela de derechos) y 11 (Comunicación de datos). En sólo una ocasión se ha sancionado la infracción del artículo 9 (Seguridad de los datos) de dicha norma.

Entre las resoluciones dictadas por el Director de la Agencia de Protección de Datos en relación con hechos constitutivos de infracción del artículo 4.3 de la LOPD, cabe reseñar sendas resoluciones sancionadoras de los procedimientos incoados a consecuencia de dos denuncias donde se pusieron de manifiesto errores cometidos por una entidad bancaria en la comunicación de datos al fichero de la Central de Información de Riesgos del Banco de España (CIRBE). Se constató, en ambos casos, que se había producido un error en dicha comunicación por lo que el Director de la Agencia de Protección de Datos acordó iniciar procedimiento sancionador a la entidad bancaria por presunta infracción del artículo 4.3 de la Ley Orgánica 15/1999, que dispone que: « *Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.»* Durante el periodo de tramitación del procedimiento sancionador, la entidad bancaria presentó, entre otras, alegaciones respecto a que la información de los datos al CIRBE está fuera del ámbito de aplicación de la LOPD. Sin embargo, aunque la Agencia ha mantenido el criterio de que el CIRBE es un fichero público, y por tanto, no regulado por el art. 29 de la LOPD *de prestación de servicios de información sobre solvencia patrimonial y crédito,* ello no implica la exclusión del resto de la Ley Orgánica 15/1999.

La Agencia de Protección de Datos ha resuelto numerosos procedimientos sancionadores por incumplimiento del principio de calidad de datos en el fichero CIRBE, tanto por altas improcedentes como por mantener la información inexacta en el mismo. En este mismo sentido, la Audiencia Nacional y el Tribunal Superior de Justicia de Madrid, han dictado sentencias en los recursos contenciosos-administrativos interpuestos por las entidades financieras sancionadas que ratifican las resoluciones impugnadas.

Así, el Tribunal Superior de Justicia de Madrid, en la Sentencia nº 322, de 21 de marzo de 2001, en el Fundamento de Derecho Tercero señala que *«(...) desde el momento en que los datos suministrados al CIRBE por las Entidades de Crédito son accesibles a éstas que pueden recabar la información que precisen para su normal desarrollo (al margen y con independencia del secreto bancario), dicha Central de Información de Riesgos presta, a juicio de esta Sala y Sección además de la función de control, un servicio —aunque limitado a las Entidades de Crédito, por lo que aquí interesa— de Información sobre solvencia Patrimonial y Crédito, y, en tal sentido, la remisión de datos relativos a la solvencia patrimonial de los clientes de las Entidades Bancarias han de cumplir las garantías y requisitos exigidos por el expresado art. 4.1.3, correspondiendo al acreedor —en este caso a la Entidad Bancaria suministradora del dato al CIRBE— la responsabilidad de la veracidad y calidad de los datos suministrados.*

Por ello, como declaran las resoluciones, después de comprobar que se había hecho uso de unos datos inexactos relativos a los denunciantes, al comunicar a la CIRBE una información errónea y no veraz sobre el riesgo asumido por aquéllos, se entendió conculcado el principio de calidad de datos.

En relación con las infracciones del artículo 10 (deber de secreto) cabe citar la resolución de un procedimiento incoado contra una entidad bancaria por vulneración del deber de secreto al haberse facilitado información sobre datos bancarios, pese a que dichos datos fueron solicitados a través de un Juzgado.

En la denuncia, se exponía que una entidad bancaria había facilitado datos a la Policía Nacional, en el transcurso de una investigación policial, sin consentimiento del afectado y sin orden judicial. En la tramitación del procedimiento quedó acreditado que el Juzgado había solicitado la información remitida a la Policía Nacional pero que la comunicada excedía de lo solicitado por el órgano judicial, por lo que, el Director de la Agencia de Protección de Datos acordó incoar procedimiento sancionador a la entidad bancaria por una supuesta infracción de artículo 10 de la LOPD.

La entidad bancaria, alegó que los hechos imputados no vulneran la normativa vigente de protección de datos, al deducirse de los mismos que su actuación se ha limitado a acatar un mandamiento del Juzgado. Sin embargo, quedó acreditado a lo largo de la tramitación del procedimiento, que el Juzgado dictó Auto acordando librar oficio a la entidad bancaria para que se presentara informe a la Policía Nacional sobre los movimientos bancarios habidos en diversas cuentas del afectado, y que la entidad bancaria extralimitándose del contenido del mandato judicial, remitió a la Policía Nacional informe relativo al movimiento de cuentas bancarias no incluidas en el citado Auto, abarcando un periodo de tiempo más amplio que el requerido por el citado Juzgado, por lo que dicho exceso de información no está amparada bajo la cobertura del artículo 11.2.d) que permite la cesión sin consentimiento cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Por ello, se apreció una vulneración del artículo 10 de la LOPD.

Así mismo, merece ser reseñada la resolución del procedimiento incoado contra una entidad financiera por vulneración del deber de secreto al quedar acreditado que dentro de la gestión de recobro llevada a cabo por la misma, se mantuvieron contactos telefónicos con vecinos del titular de la cuenta en la que existen impagados, así como con sus familiares. En el primer caso, no se facilitaba información acerca de la existencia de la deuda, sino que se les rogaba con amabilidad que informaran al deudor para que se ponga en contacto con ellos. Sin embargo, a los familiares más cercanos se les informaba de la deuda, incluyendo en el fichero de la entidad la información facilitada por ellos.

La resolución establece que esta actuación incumple lo preceptuado en el artículo 10 de la LOPD al facilitar datos a familiares sobre el impago de una deuda, vulnerándose así, el secreto profesional respecto de estos datos.

En relación con la vulneración del deber de secreto, cabe mencionar también la resolución del procedimiento incoado a una entidad bancaria a consecuencia de la remisión por ésta, de diversos faxes conteniendo datos de la persona denunciante de los hechos, a un tercero. Durante el procedimiento quedó acreditado que el hecho se reiteró en varias ocasiones y que el representante de la empresa que recibió los faxes lo comunicó a la entidad bancaria hasta en ocho ocasiones.

La entidad financiera alegó en su defensa que los hechos que se le imputan ocurrieron por error. La alegación es rechazada en la resolución ya que la conducta de la entidad bancaria no se produce de forma puntual, sino reiterada, y pese a haber sido advertida en varias ocasiones por el receptor de los faxes. Concurre, por tanto, en la entidad imputada una reiterada falta de diligencia exigible, suficiente para apreciar y declarar la infracción.

Respecto de la vulneración de los artículos 11 (Comunicación de Datos) y 6 (Consentimiento del afectado) cabe destacar dos resoluciones del Director de la Agencia. En ellas, con motivo de un contrato suscrito entre dos entidades bancarias por el cual una de ellas cedía el negocio bancario de diferentes oficinas a la otra entidad, se envió a los clientes, como paso previo al traspaso de sus datos a la entidad bancaria de destino, un *mailing* en el que se les informaba de la comunicación de sus datos personales y del traspaso de sus cuentas. En ese escrito se les solicitaba el consentimiento para dicha cesión, informando que, de no recibir respuesta en un plazo de quince días se entendería que prestaba efectivamente dicho consentimiento. Sin embargo, en el transcurso de las actuaciones practicadas por la Inspección de Datos no se encontraron evidencias suficientes que permitieran acreditar que a los denunciantes se les había notificado con anterioridad que sus datos personales iban a ser comunicados a la otra entidad. Por ello, el Director de la Agencia de Protección de Datos acordó iniciar procedimiento sancionador a la entidad bancaria que ha comunicado los datos por la presunta infracción del artículo 11.1 de la Ley Orgánica 15/1999 a la entidad receptora de los mismos por presunta infracción de artículo 6.1 de dicha norma.

Ambas entidades basan sus alegaciones en afirmar la legalidad de la cesión de negocio bancario. Sin embargo, la cuestión que se dilucida en ambos procedimientos y que justifica la intervención de la Agencia de Protección de Datos es que la referida relación contractual entre ellas —cuya legalidad mercantil no se pone en duda— implica una comunicación de datos personales que debe ser examinada a efectos de comprobar si cumple con las garantías que exige la L.O. 15/1999.

La L.O. 15/1999 recoge el principio del consentimiento en su artículo 6, exigiendo para el tratamiento de los datos de carácter personal el consentimiento inequívoco del interesado. De acuerdo con la definición de tratamiento que la misma Ley recoge en su artículo 3 c), las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias deben ser consideradas como tratamiento de datos.

En consecuencia, lo que procedía examinar en estos casos es si la entidad cedente tenía el consentimiento inequívoco de los interesados para la cesión de sus datos a consecuencia del contrato de cesión de negocio bancario y si la entidad cesionaria se aseguró de la existencia del consentimiento de los interesados para poder tratar sus datos.

Durante la tramitación de los procedimientos se constató la realización de un *mailing* para informar de la comunicación de datos personales, del traspaso de cuentas y de la solicitud del consentimiento para dicha cesión, informando que de no recibir respuesta en un plazo de quince días prestaba efectivamente dicho consentimiento. La resolución admite que puede ser válida la obtención del consentimiento tácito de los clientes, pero para acreditar que dicho consentimiento realmente es *inequívoco* la entidad cedente debía acreditar que cada cliente había recibido la referida carta Así se aseguraba que, de no recibir contestación de los clientes, ya había obtenido ese consentimiento de forma tácita.

La resolución cita la Sentencia de la Audiencia Nacional número 103/1999, de fecha 14 de abril de 2000 (referida a la obtención del consentimiento de conformidad con lo establecido en la Ley Orgánica 5/1992), en cuyo Fundamento de Derecho Séptimo señala que: «*tampoco puede admitirse, ..., la existencia de un consentimiento tácito o impropiamente llamado «silencio positivo» del afectado para admitir la cesión de sus datos, pues tal forma de obtener el consentimiento requeriría, en la mejor de las hipótesis, una rigurosa constancia documental de que la entidad cedente había informado y conservaba el escrito, con constancia de la recepción por el interesado...».* También hace referencia a la Sentencia de la Audiencia Nacional número 121/1999, de 7 de julio de 2000, que recoge en el Fundamento de Derecho Tercero que: «*Estos hechos están admitidos por XXXXX y opone en su defensa que había recabado de sus clientes el consentimiento para la cesión de sus datos en comunicación remitida a todos por vía ordinaria advirtiéndoles que de no mediar oposición expresa, se considerarían legitimadas para la cesión. Este tema del consentimiento tácito ha de ser tratado con una gran delicadeza cuando están en juego derechos constitucionales básicos, (art. 18-4 C.E.) y a ello tiende toda la regulación legal contenida en el articulado de la L.O. 5/92 y su explicación y filosofía recogida en la Exposición de Motivos. En la vida de relación es muy posible reconocer formas de tácita aceptación, pero siempre en aspectos no trascendentales o cuando se está operando sobre situaciones consolidadas y que están en la común consideración a modo de valores entendidos. No es el caso cuando lo que está en juego es la privacidad de las personas de ahí todas las cautelas normativas tendentes a proteger esa privacidad, sin que quepan interpretaciones de laxitud del art. 11-1 de la Ley a menos que el titular de la intimidad se haya situado voluntariamente en situación de abandono de la defensa de ese derecho, en cuyo caso sí podría hablarse de una forma de consentimiento tácito. Pero hay más, y es que ni tan siquiera consta que los denunciantes hayan recibido ninguna comunicación que se dice hecha por correo ordinario y cuya recepción se niega e incluso de ser cierta sería más que dudosa su eficacia sustitutoria del consentimiento»*

En el caso enjuiciado no se había acreditado que el referido envío solicitando el consentimiento fuese notificado a los denunciantes con anterioridad a que sus datos personales fuesen comunicados a la otra entidad bancaria.

Por ello se declara que la entidad cedente realizó una comunicación de los datos de clientes sin haber obtenido su consentimiento infringiendo el artículo 11.1 de la L.O. 15/1999. Asimismo se declara que la entidad cesionaria está obligada a la observancia de las disposiciones de la citada Ley debiendo asegurarse de que existe consentimiento de los interesados para que su entidad pueda tratar sus datos personales. Sin embargo, al no verificar la forma de obtención del consentimiento y valorar si se habían cumplido las estipulaciones de la L.O. 15/1999 es sancionada por tratamiento de datos sin el consentimiento de los afectados.

Finalmente debe destacarse una resolución de archivo en relación a la información suministrada al fichero de la Central de Información de Riesgos del Banco de España (CIRBE).

Se recibió una denuncia donde se ponía de manifiesto la inclusión de los datos personales de un afectado en el fichero CIRBE motivada por un préstamo hipotecario que finalmente no fue suscrito. Las actuaciones inspectoras permitieron comprobar que el denunciante efectivamente había solicitado una operación hipotecaria que fue aprobada por la entidad bancaria. De acuerdo con lo dispuesto en la Circular 3/1995 del Banco de España, las entidades bancarias tienen obligación de notificar a la CIRBE las operaciones de riesgo que asuman, considerando entre ellas los préstamos o créditos de dinero que concedan, tanto en su modalidad de disponible como de dispuesto. En consecuencia, en el momento en que se aprueba la concesión del crédito, la entidad bancaria debe declarar la información a la CIRBE como crédito disponible.

Esta obligación de notificación de crédito disponible encuentra su justificación en la necesidad de conocer la información requerida a los efectos de la elaboración de estadísticas, la disciplina bancaria y la dirección de la política del crédito —finalidades previstas para la CIRBE en el Decreto Ley 18/1962 que estableció su creación—, sin que en este caso la referida Central de Riesgos actúe como uno de los ficheros previstos en el artículo 29.2 de la Ley Orgánica 15/1999, esto es, prestando información sobre el incumplimiento de obligaciones dinerarias.

Por ello, la entidad financiera actuó conforme establecen las normas del Banco de España archivándose las actuaciones.

4.7. Tratamiento de datos personales en otros sectores de actividad

A lo largo del año 2002 el Director de la Agencia de Protección de Datos ha firmado varias resoluciones en las que se hayan implicadas empresas cuyo sector de actividad no se puede

encuadrar en los apartados enumerados anteriormente. Una de estas resoluciones acuerda el archivo de actuaciones y el resto son resoluciones declarativas de infracciones de la LOPD.

A continuación se expone un breve resumen de aquellas resoluciones de procedimientos sancionadores que, por su novedad, pueden resultar interesantes:

- En dos resoluciones están implicadas empresas que ofertan a las personas implicadas en un accidente de tráfico, los servicios de asesoramiento, gestión y reclamación de daños y perjuicios ante la autoridad judicial correspondiente. Los denunciantes manifiestan, en ambos casos, que tras sufrir un accidente de tráfico en el que únicamente se había personado la Policía Local y los servicios asistenciales, reciben, en sus domicilios particulares, llamadas telefónicas de las empresas citadas ofreciéndoles, por un módico precio, los servicios citados anteriormente. Incluso una de ellas remitió una carta personalizada a una accidentada.

  En ambos casos se probó que las citadas empresas habían incorporados los datos personales de los accidentados en sus ficheros informáticos y, sin embargo, ninguna de ellas pudo acreditar cuál fue el origen de la información utilizada. Este hecho motivo que el Director resolviera imponer sanciones a ambas empresas por tratar los datos personales de los accidentados sin su consentimiento.

- En otro supuesto, la resolución impone una sanción a un concesionario de coches y a su entidad financiera. En este caso, el hecho denunciado se centra en el uso indebido que hace el concesionario de la información relativa a uno de sus clientes, la cual había sido extraída de los ficheros informáticos cuyo responsable es la financiera.

  El concesionario actúa como agente comercial de la financiera por lo que, a aquellos clientes que solicitan la financiación del vehículo que van a adquirir, el concesionario les ofrece la posibilidad de gestionarlo a través de su financiera. El concesionario dispone de un terminal conectado a la central de la financiera que utiliza para introducir los datos del cliente relativos a la propuesta de financiación así como para consultar el estado de las propuestas que ha efectuado.

  Cuando las propuestas de financiación son rechazadas por la entidad financiera, queda una anotación en su fichero comentando el motivo del rechazo. En este caso concreto, la anotación hace referencia a información obtenida por la financiera del fichero Asnef, fichero al que la entidad tiene acceso en virtud de un contrato suscrito con Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, S.L..

  Aunque la inspección de datos comprobó que el comentario incluido por la entidad financiera en su fichero informático no había sido incluido por el concesionario en su

fichero informático de clientes, este último utilizó una copia impresa de la información contenida en el fichero de la entidad financiera para acompañarlo como documentación justificativa, en su propia defensa, en un proceso iniciado en una Junta Arbitral de Consumo.

Respecto de la entidad financiera, el Director también resuelve imponer una sanción a la misma por ceder datos personales al concesionario ya que, queda probado que el concesionario ha accedido al fichero de la financiera y concretamente ha extraído en soporte papel información de los comentarios relativos al motivo por el cual la financiera rechaza la propuesta de financiación efectuada por el concesionario.

La persona solicitó la financiación de la entidad financiera y, por tanto, es lógico que ésta, en el ámbito de su actividad, emita una contestación al concesionario sobre la aprobación o no de la financiación. Sin embargo la financiera contestó al concesionario con datos sobre la calidad y cuantía de la incidencia así como con datos personales de la afectada, que no se encuentran relacionados con las funciones legítimas del cesionario y, por ello, necesitaban del consentimiento de la afectada.

Dado que el concesionario y la entidad financiera no habían suscrito ningún contrato escrito que regulase la relación existente entre ambas entidades, el Director resolvió imponer una sanción por infracción del artículo 11 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Finalmente, el Director impuso una sanción a una agencia de publicidad por no tener inscrito su fichero informático en el Registro General de Protección de Datos. El escrito que inició las actuaciones inspectoras fue presentado en la Agencia por la Fiscalía de un Tribunal Superior de Justicia, que manifestaba que se habían encontrado en un contenedor de obras fichas que contenían datos personales, en su mayoría, de menores de edad y aportaba los originales citados. El hecho de permanecer las fichas en un contenedor de obras viene producido por el traslado de oficinas de la agencia de publicidad.

  Aunque se trataba de fichas que contienen los datos personales de forma manuscrita facilitados por los padres de los menores o por los propios interesados, posteriormente la agencia de publicidad los había tratado automatizadamente incorporándolos a sus bases de datos y creando un fichero automatizado que, debió haber sido notificado al Registro General de Protección de Datos. La omisión de esta obligación legal determinó la declaración de la infracción tipificada en el artículo 44 c) de la LOPD.

IV. La Secretaría General

1. Gestión de Personal

Las funciones conducentes a proporcionar y administrar los medios personales y materiales para el funcionamiento de la Agencia de Protección de Datos, así como las competencias relativas al Servicio de Atención al Ciudadano, las atribuye el EAPD a la Secretaría General. Así se puso de manifiesto en esta Memoria Anual en su epígrafe III, 2.5, de la parte correspondiente a la Estructura y Funcionamiento de la Agencia.

Durante el Ejercicio 2002 la plantilla máxima de la APD, autorizada por la CECIR en el año 2001, ha permanecido invariable. Es decir, consta de 68 funcionarios de la Administración General del Estado y 2 laborales. Así mismo presta servicios en la APD el Abogado del Estado Jefe de Gabinete Jurídico que, sin embargo, desde noviembre de 2001 pasó a depender de la Relación de Puestos de Trabajo del Servicio Jurídico del Estado.

A pesar de esta invariabilidad de la plantilla de la APD, no se puede deducir que durante 2002 no se hiciera gestión alguna en orden a mejorar las condiciones retributivas de los funcionarios, dada la escasa receptividad que tuvo en la CECIR la modificación de la Relación de Puestos de trabajo acometida en 2001. A tal fin, por escrito del Director, de fecha 31 de julio de 2002, se elevó a la Dirección General de Costes de Personal y Pensiones Públicas una propuesta de aumento de masa de productividad o, alternativa-

mente, de productividad por objetivos. Sin embargo, lamentablemente, esta iniciativa no tuvo éxito.

El nuevo Director de la APD, que fue nombrado en noviembre de 2002, solicitó comparecer a petición propia ante la Comisión Constitucional del Congreso de los Diputados para exponer sus proyectos de futuro. Dentro de su intervención se refirió a las dificultades con que se encontraba la Agencia al no contar de inmediato con una ampliación de su Relación de Puestos de Trabajo. En este sentido el Director dio instrucciones a la Secretaría General para que elaborase una propuesta de modificación de la Relación de Puestos de Trabajo de la APD que remediara el creciente aumento de la carga de trabajo y la hiciera compatible con el objetivo de Estabilidad Presupuestaria, con idea de presentarla ante la CECIR durante el primer semestre de 2003.

No obstante, durante 2002 se han realizado las labores tradicionales para la provisión de puestos de trabajo que habían quedado vacantes. En este sentido, se publicaron y adjudicaron las siguientes:

- Resolución de 13 de febrero de 2002, por la que se resuelve el concurso específico convocado por Resolución de 13 de diciembre de 2001. En esta Resolución se cubrieron tres niveles 18, dos en el RGPD y uno en la Secretaría General, y un nivel 14 también en Secretaría General, quedando desiertas dos plazas de Auxiliar de Informática en la SGID.

- Resolución de 15 de marzo de 2002, por la que se resuelve el concurso específico convocado por Resolución de 12 de noviembre de 2001. Se cubrieron un nivel 28 de Inspector de Datos, tres niveles 26 de Subinspectores de Datos, y dos plazas en Secretaría General, una de nivel 26 y otra de 24.

- Resolución de 15 de marzo de 2002, por la que se resuelve la adjudicación por libre designación del puesto de Subdirector General de Inspección de Datos, que fue convocado por Resolución de 24 de enero de 2002.

- Resolución de 10 de mayo de 2002, por la que se resuelve la adjudicación por libre designación del puesto de Adjunto al Director, que fue convocado por Resolución de 4 de abril de 2002.

- Resolución de 19 de julio de 2002, por la que se resuelve el concurso específico convocado por Resolución de 5 de abril de 2002. Se cubrieron dos plazas de Auxiliar de Informática nivel 14, una de la SGID y otra en la Secretaría General.

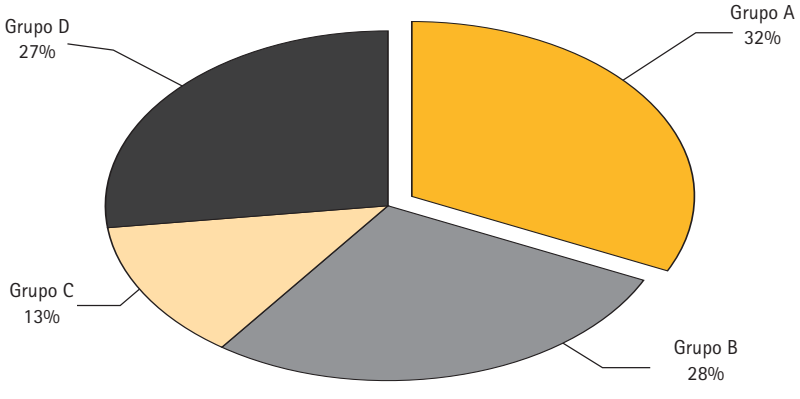
- Resolución de 1 de agosto de 2002, por la que se resuelve el concurso específico convocado por Resolución de 31 de mayo de 2002, para cubrir un puesto de Inspector de Datos.

- Resolución de 28 de octubre de 2002, por la que se resuelve el concurso específico convocado por Resolución de 12 de julio de 2002, por la que se cubrieron una plaza de nivel 28, Jefe de Área de Atención al Ciudadano, y una de nivel 26, de Inspector-Instructor.

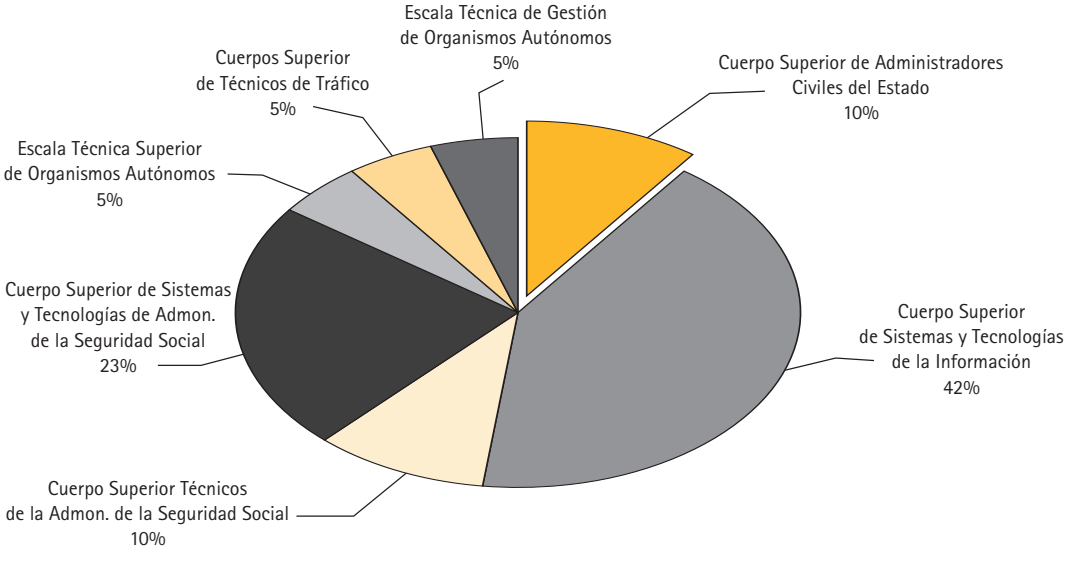
En total se cubrieron diecisiete plazas que, en diferentes momentos de 2002, se encontraban vacantes.

La dimensión y composición de la plantilla de la Agencia, a 31 de diciembre de 2002, es la que se deriva de los siguientes gráficos:

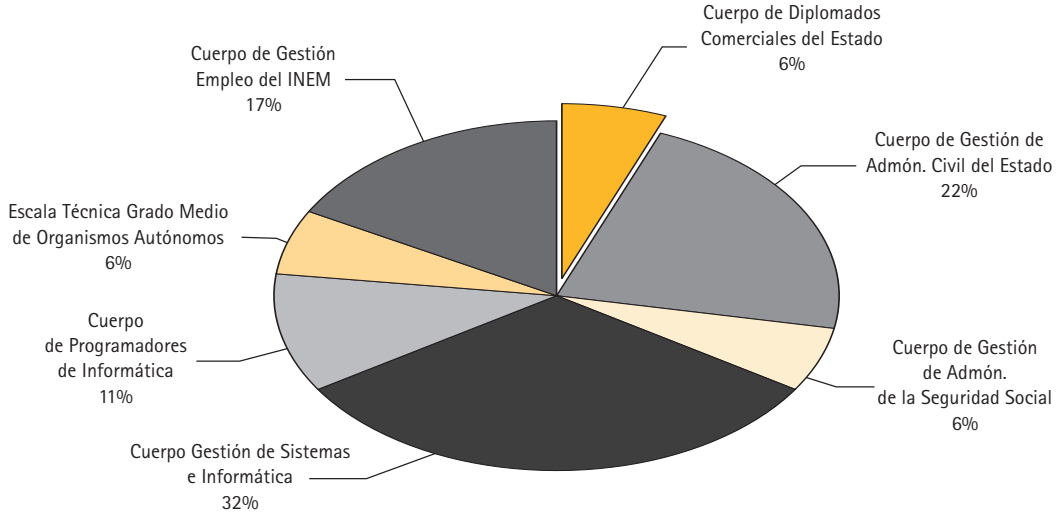
DISTRIBUCIÓN POR GRUPOS DE CLASIFICACIÓN DE FUNCIONARIOS



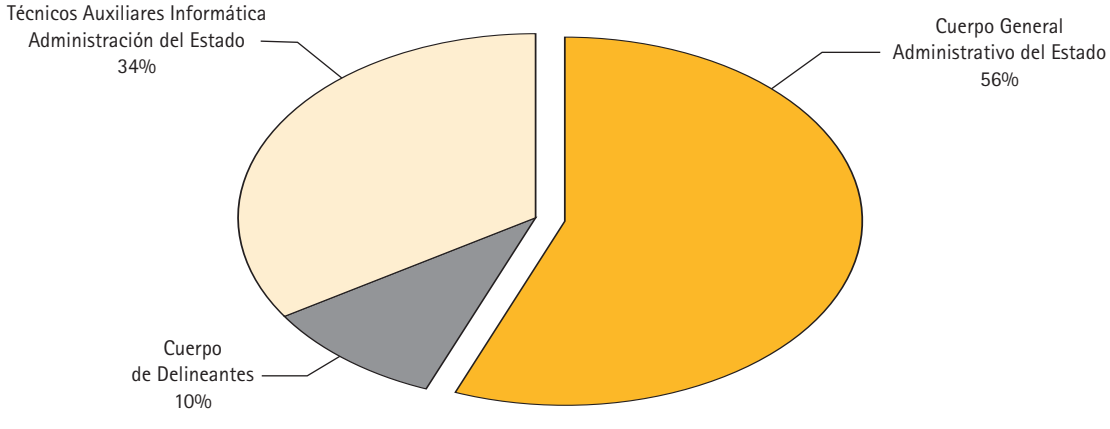
DISTRIBUCIÓN POR CUERPOS DEL GRUPO DE CLASIFICACIÓN A



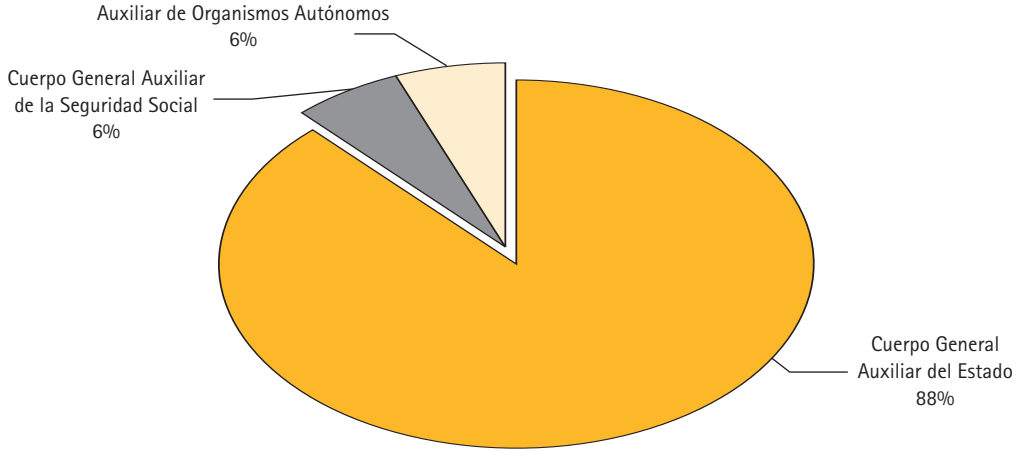
DISTRIBUCIÓN POR CUERPOS DEL GRUPO DE CLASIFICACIÓN B



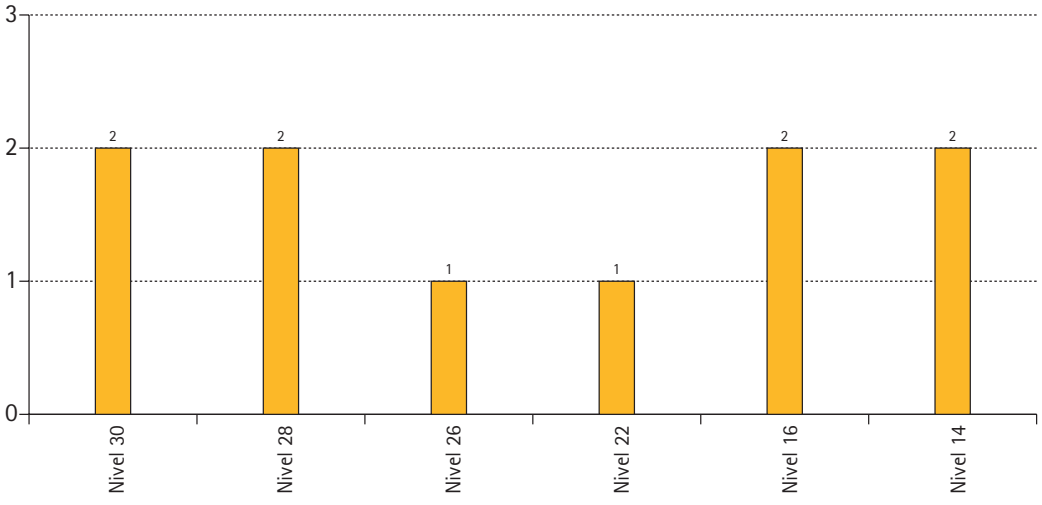
DISTRIBUCIÓN POR CUERPOS DEL GRUPO DE CLASIFICACIÓN C



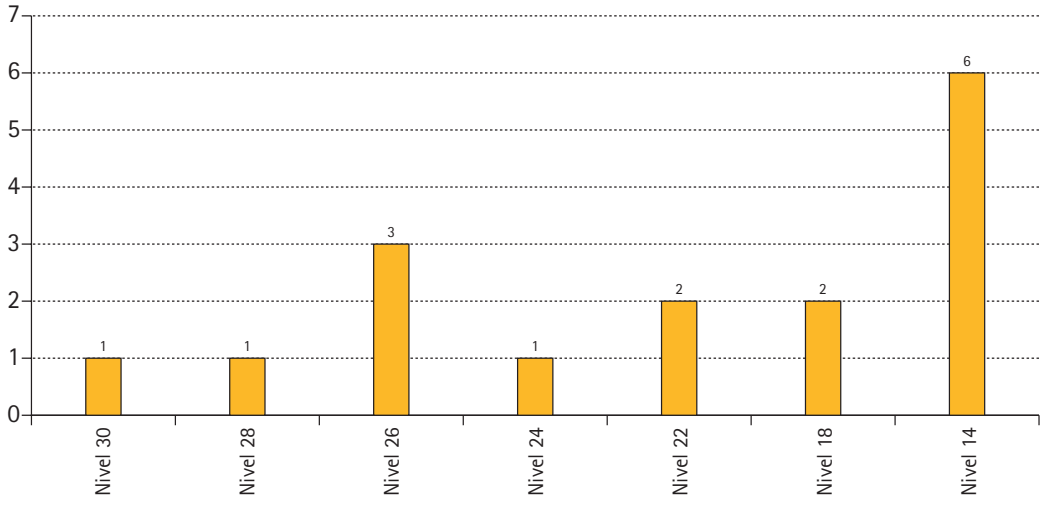
DISTRIBUCIÓN POR CUERPOS DEL GRUPO DE CLASIFICACIÓN D



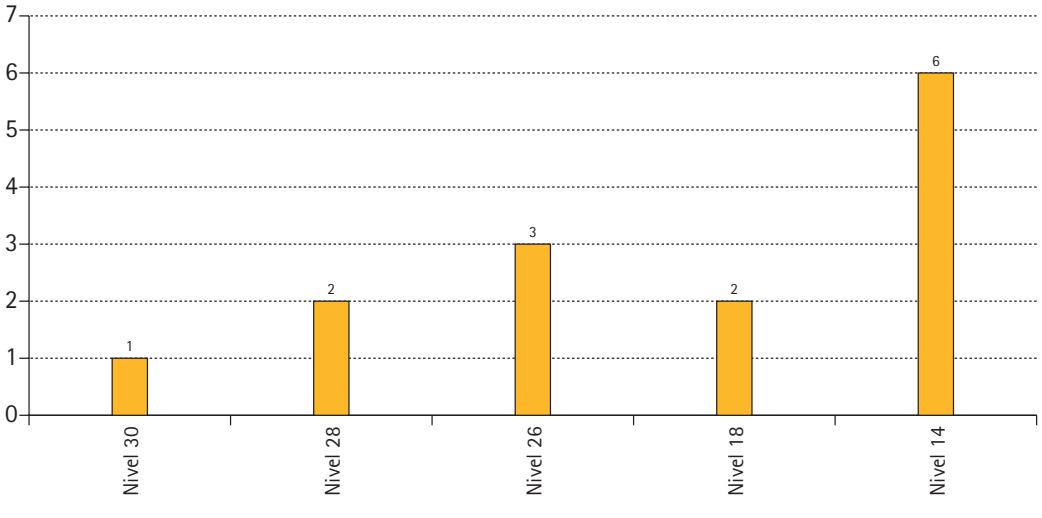
UNIDAD DE APOYO AL DIRECTOR POR NIVELES



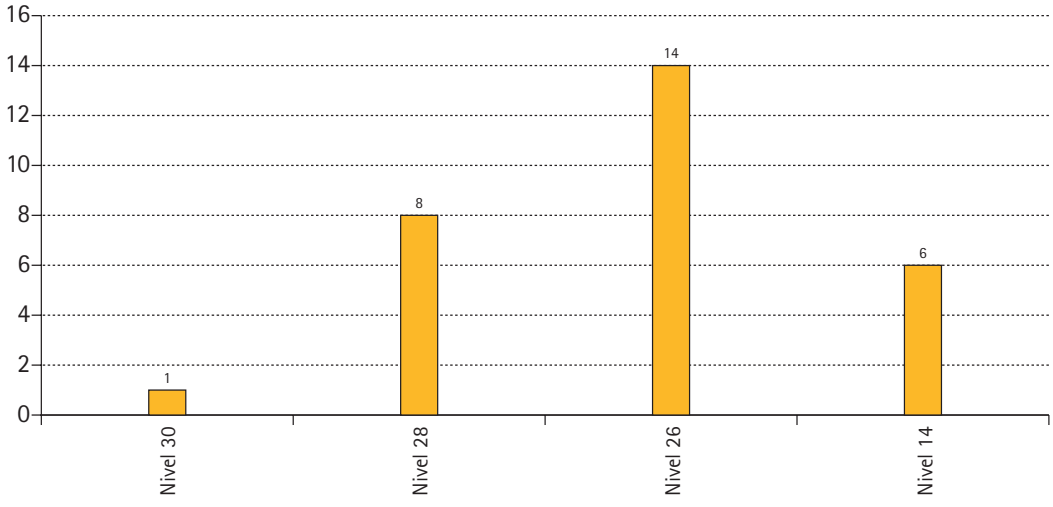
SECRETARÍA GENERAL POR NIVELES



REGISTRO GENERAL POR NIVELES



INSPECCIÓN DE DATOS POR NIVELES

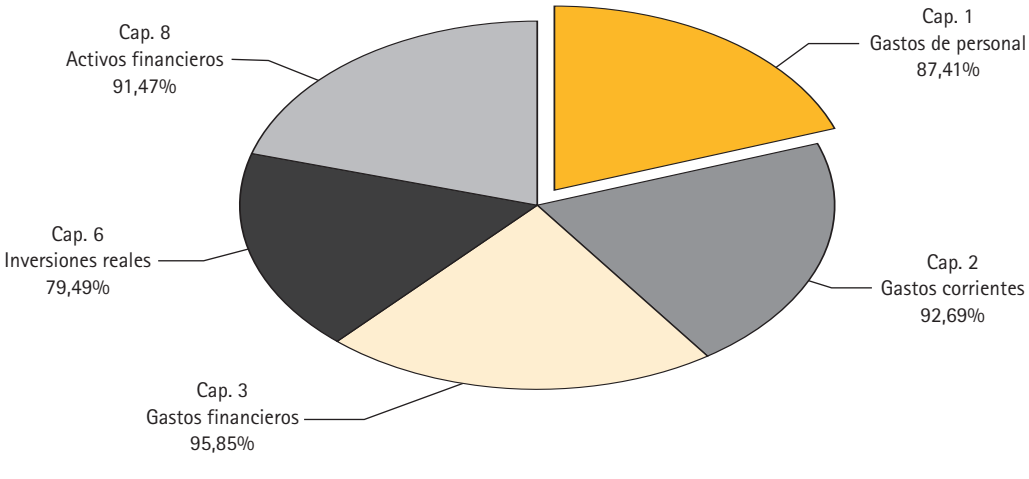


2. Gestión Económico-Financiera y Presupuestaria

De acuerdo con las funciones que el EAPD atribuye a la Secretaría General, y que ya han quedado reflejadas en esta Memoria al analizar el epígrafe III, 2.5 de la parte dedicada a la Estructura y Funcionamiento de la Agencia de Protección de Datos, se han llevado a cabo las siguientes tareas:

- Ejecución y seguimiento presupuestario. El grado de realización del Presupuesto de Gastos de la APD para el Ejercicio 2002 es el que se expresa en el siguiente gráfico:

EJECUCIÓN PRESUPUESTARIA 2002



- Modificaciones Presupuestaria:
  Durante en ejercicio 2002 se produjeron las siguientes ampliaciones de crédito:

  13.301.160.00 por un importe de 45.955 €.
  13.301.226.03 por un importe de 215.402,28 €.

- Gestión del presupuesto de ingresos de la Agencia en lo relativo al concepto 391.02 «*Multas y sanciones*», 400 «*Transferencias corrientes*», 520.99 «*otros ingresos de cuentas bancarias*», 700 «*transferencia de capital*», y 870 «*Remanente de Tesorería*».

- Rendición de Cuentas Anuales, cuyo resumen fue publicado por Resolución del Director de la Agencia de Protección de Datos de 10 de octubre de 2002 (B.O.E. nº 260, de 30 de octubre de 2002).

- Actualización del inventario de bienes y derechos que integran el patrimonio de la Agencia.

- Gestión administrativa de la Biblioteca de la Agencia.

3. Otras Actividades de Gestión Administrativa

Dentro del ámbito negocial llevado a cabo por la Secretaría General, en virtud de la delegación de esta competencia contractual en el Secretario General, por Resolución del Director de la Agencia de Protección de Datos de 24 de abril de 1998, se han adjudicado los siguientes contratos:

- 2 expedientes de contratación de más de 30.050,60 euros que se imputaron a las aplicaciones presupuestarias 13.301.226.02 (Publicidad y Propaganda), y 13.301.227.06 (Estudios y Trabajos Técnicos).

- 243 expedientes de Contratación de contratos de importe inferior a 30.050.60 euros. Por orden decreciente de importancia los expedientes se imputaron a las siguientes aplicaciones presupuestarias:

  — 51 expedientes a la 13.301.620.
  — 25 expedientes a la 13.301.220.00.
  — 25 expedientes a la 13.301.220.01.
  — 24 expedientes a la 13.301.227.06.

— 22 expedientes a la 13.301.226.01.
— 20 expedientes a la 13.301.226.01.
— 12 expedientes a la 13.301.216.
— 11 expedientes a la 13.301.226.06.
— 10 expedientes a la 13.301.215.
— 9 expedientes a la 13.301.220.02.
— Resto (34 expedientes) a las aplicaciones presupuestarias: 212, 213, 222.00, 202, 221.12, 240, 221.99, 222.04, 227.00, 162.05, 162.09, 221.00, 222.01, 223, 226.03 y 227.01.

Por lo que se refiere al número total de notificaciones de resoluciones del Director de la Agencia de Protección de Datos, durante el año 2002 se mantuvieron en número sensiblemente inferior a las cifras del año 2001. Concretamente se realizaron un total de 1.108 en expedientes finalizados y 807 en expedientes aún abiertos, es decir, se efectuaron 1.915 notificaciones en 2002.

En cuanto al número de asientos del Registro General de la Agencia de Protección de Datos, la evolución de los datos de 2002 (45.786 registros) arroja un incremento del 63,33 por ciento sobre los 28.034 producidos en 2001. De los 45.786 señalados, 38.598 registros corresponden a registros de entrada y 7.188 a registros de salida.

Así mismo, durante el año 2002 se procedió a convocar el *Premio Agencia de Protección de Datos*, VI Edición, y el *Premio de Periodismo Agencia de Protección de Datos*, III Edición. Con fecha 3 de diciembre de 2002, el Jurado compuesto por el Consejo Consultivo acordó por unanimidad fallar ambos premios del siguiente modo:

- *Premio Agencia de Protección de Datos* al trabajo titulado «*Transferencia Internacionales de Datos Personales*», del que es autora Doña Diana Sancho Villa.

- También el Jurado decidió conceder una Accésit al trabajo titulado «*Tratamiento de Datos Personales en el ámbito sanitario: intimidad versus interés público (especial referencia al SIDA, técnicas de reproducción asistida e información genética)*», del que es autora Doña Noelia de Miguel Sánchez.

- Respecto del Premio de Periodismo Agencia de Protección de Datos, el Jurado decidió, por unanimidad, declararlo desierto, a tenor de lo previsto en la Base Séptima de la Convocatoria.

En lo relativo a la organización de conferencias y seminarios, la Secretaría General organizó el *I Encuentro Iberoamericano de Protección de Datos Personales*, en Cooperación con la Agencia de Protección de Datos de la Comunidad de Madrid. El encuentro tuvo lugar los días 20 y 21 de mayo de 2002, y se desarrolló en San Lorenzo de El Escorial (Madrid).

4. Área de Atención al Ciudadano

4.1. Actividad desarrollada

La 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 los datos de carácter personal. Esta función viene atribuida a la SGAPD por el artículo 31.d) del EAPD.

Este 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 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 aplicable en esta materia.

En función de las diferentes formas en que se presta la Atención al Ciudadano, se pueden distinguir, en primer momento, la atención personalizada que a lo largo del año 2002 ha representado un total de 24.235 consultas, y la información que obtienen los ciudadanos directamente a través de la página Web de la Agencia y cuyo desglose se analizará más adelante.

Por lo que se refiere a la atención personalizada, se viene realizando, de tres formas distintas: 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 2002 y se desglosa por las modalidades citadas:

Atención telefónica	Atención presencial	Atención por escrito	Total
18.870	2.722	2.643	24.235

Como referencia comparativa, durante el año 2001 el número de consultas por modalidades fue el siguiente:

Atención telefónica	Atención presencial	Atención por escrito	Total
15.634	1.890	2.416	19.940

Se puede señalar que la atención personalizada al ciudadano en 2002 ha sido superior a la prestada en el año 2001, lo que representa un incremento de un 21,54%. Este incremento global se explica del siguiente modo: Respecto de la atención telefónica sigue una línea creciente, pasando de 15.634 consultas en el año 2001 a 18.870 en el año 2002, lo que implica un incremento de actividad del 20,69%. La atención presencial en la sede de la Agencia ha aumentado en casi un 44,02% respecto del año anterior, habiendo también aumentado, la atención a consultas escritas en un 9,40%.

Por lo que se refiere a la información obtenida a través de la página Web de la APD, se destaca que, en la misma 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 2002 como fruto de una inspección de oficio dirigida al sector.
- La legislación relativa a la protección de datos de carácter personal.
- Los modelos de cuestionarios para notificar la inscripción de ficheros, tanto de titularidad pública como privada, al RGPD.
- 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 en el año 2001 y que, como se detallará más adelante, ha supuesto una importante fuente de información para el ciudadano.

En el siguiente cuadro se concreta el detalle del número total de accesos que ha tenido la Web de la APD durante el año 2002.

NÚMERO TOTAL DE ACCESOS A LA PÁGINA WEB DURANTE EL AÑO 2002

Enero	132.031
Febrero	145.649
Marzo	136.656
Abril	158.317
Mayo	139.382
Junio	205.435
Julio	189.000
Agosto	122.356
Septiembre	211.816
Octubre	12.557
Noviembre	246.806
Diciembre	206.065
Total	**1.906.070**

En el siguiente cuadro se refleja la evolución de los accesos a la Web de la APD desde el año 1998, en que se implantó, hasta el año 2002. Por lo que se refiere a la comparativa 2001-2002, se observa un considerable incremento de esta forma de obtener información, pasando de un total de 1.572.738 a un total de 1.906.070 accesos en 2002, es decir un incremento de un 21,19 por ciento.

EVOLUCIÓN DEL NÚMERO DE ACCESOS A LA WEB DE LA AGENCIA

Año	N.º de accesos
1998	216.000
1999	506.362
2000	1.173.056
2001	1.572.738
2002	1.906.070

Respecto al apartado de consultas más frecuentes de la Web, creado en el año 2001 con el objetivo de facilitar el acceso directo a aquellas consultas que eran solicitadas con mayor frecuencia por los ciudadanos, dicho objetivo se ha visto cumplido a lo largo de los años 2002 y 2003 de forma considerable, tal y como se desprende de los siguientes cuadros, en los que se recoge el número total de accesos por consultas concretas y por meses, abarcando los meses de enero a diciembre de 2002.

NÚMERO TOTAL DE ACCESOS POR CONSULTAS CONCRETAS (ENERO-DICIEMBRE 2002)

Publicidad	8.240
Facturación Telefónica	4.854
Guías Telefónicas	4.342
Ámbito de la LOPD	6.244
Derecho de acceso	4.285
Derecho de acceso ante la APD	4.937
Ficheros de Morosos	6.431
Ficheros de Morosos con datos de fuentes públicas	2.504
Direcciones Ficheros Morosos	3.723
Inscripción ficheros	9.005
Como se deben declarar ficheros	10.017
Presentación documento seguridad	7.942
Seguridad (fichero nóminas)	8.610
Seguridad (datos de hacienda pública)	3.932
Seguridad (servicios financieros)	3.733
Implantación medidas seguridad de nivel medio	6.783
Sentencia Tribunal Constitucional sobre LOPD	6.828
Total	**102.410**

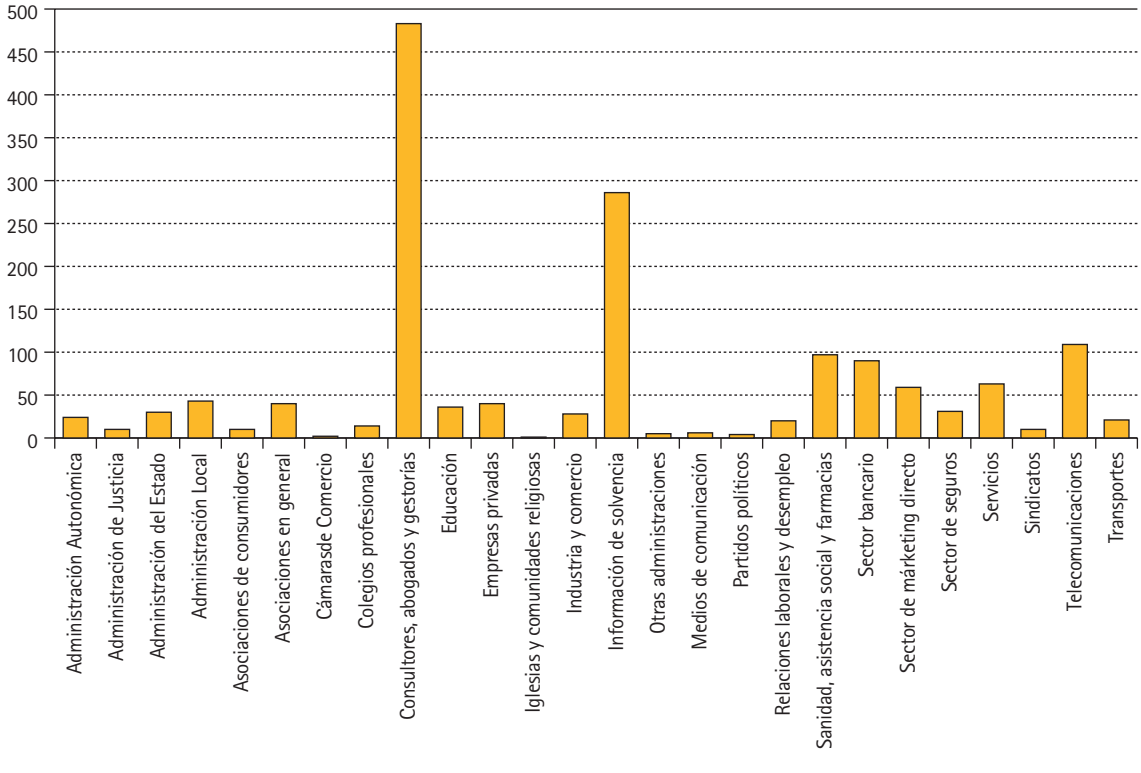
NÚMERO TOTAL DE ACCESOS *POR MESES* (ENERO-DICIEMBRE 2002)

Enero	5.719
Febrero	6.899
Marzo	6.227
Abril	7.738
Mayo	9.075
Junio	10.394
Julio	8.162
Agosto	4.627
Septiembre	8.905
Octubre	12.688
Noviembre	12.751
Diciembre	9.225
Total	**102.410**

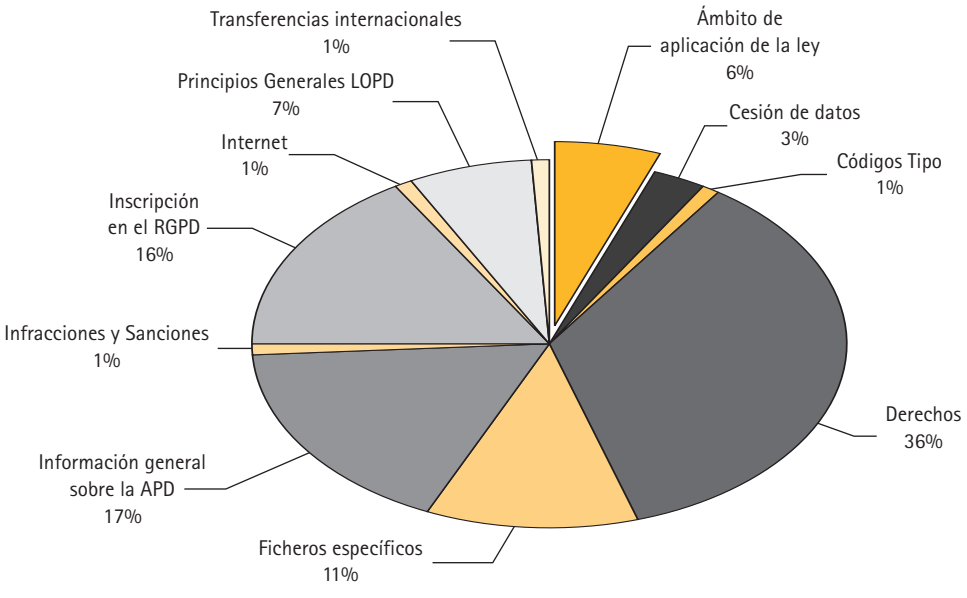
A la vista de los cuadros anteriores se puede deducir que octubre y noviembre de 2002 fueron los meses en los que más consultas se plantearon. Respecto a la materia que más interesó en 2002, fue la relativa a la inscripción de ficheros.

Seguidamente, se procede a insertar una serie de gráficos, en los que se refleja la distribución de consultas planteadas en 2002 por sectores y temas;

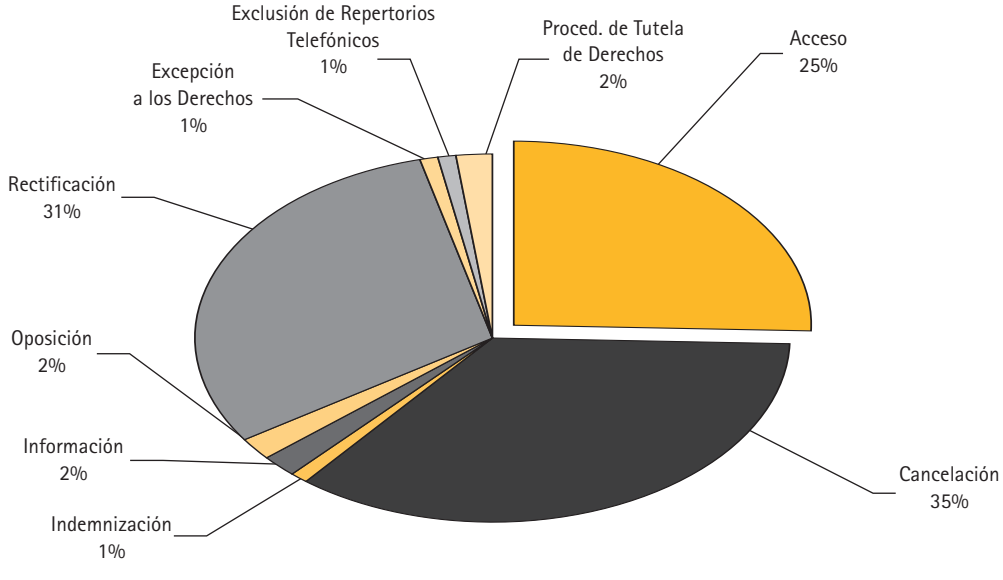
CONSULTA POR SECTORES 2002



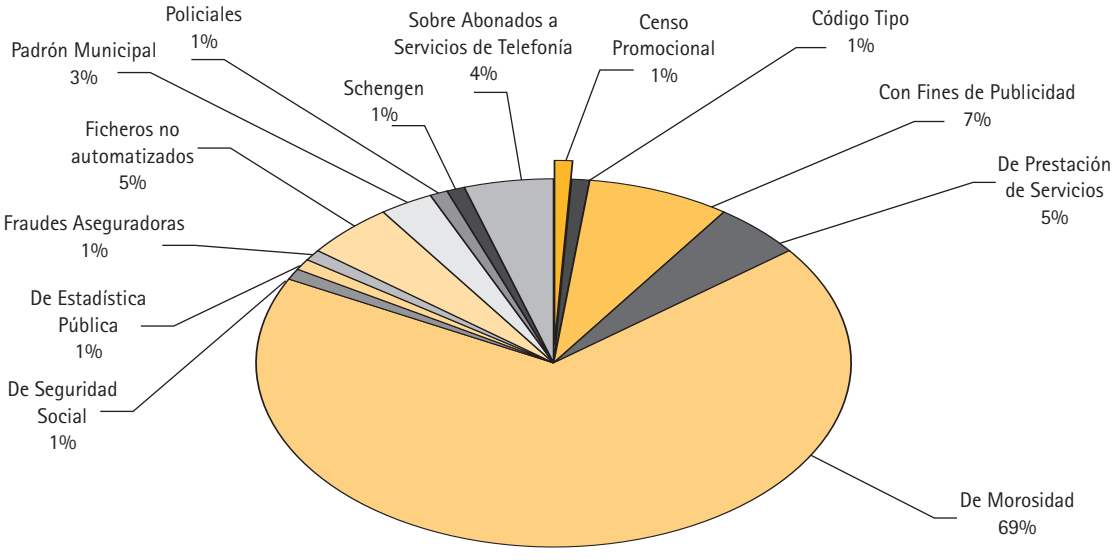
CONSULTA POR TEMAS 2002



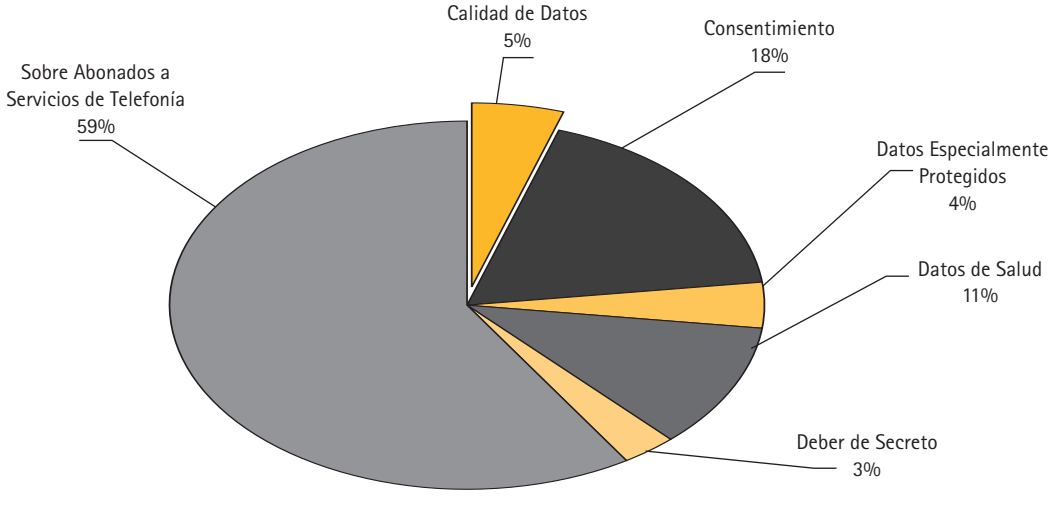
TIPOS DE CONSULTAS SOBRE DERECHOS 2002



CONSULTAS SOBRE FICHEROS ESPECÍFICOS 2002



CONSULTAS SOBRE PRINCIPIOS GENERALES DE LA LOPD 2002



4.2. Repertorio de Consultas

A continuación, y siguiendo la pauta mantenida en Memorias de años anteriores, se hará referencia a las consultas que se han considerado de mayor interés, haciendo una mención especial a las relativas a la aplicación y desarrollo del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad para Ficheros Automatizados que contengan Datos de Carácter Personal, teniendo en cuenta que por Resolución del Subsecretario de Justicia de 22 de junio de 2001, que publica el Acuerdo del Con-

sejo de Ministros de la misma fecha, se amplió el plazo de implantación de las medidas de seguridad de nivel alto hasta el 26 de junio de 2002.

4.2.1. *Responsable de los ficheros de las Comunidades de Propietarios*

En esta consulta se planteaba la cuestión de quién debía ser considerado responsable de los ficheros de las Comunidades de Propietarios y cuál era la consideración jurídica del Administrador de dichas comunidades desde la perspectiva de la protección de datos de carácter personal. La respuesta a la mencionada consulta fue la siguiente:

«Para contestar a la consulta en primer lugar habrá que analizar quien es el responsable del fichero de todos los propietarios de la Comunidad. En este sentido tal y como establece el artículo 3 d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, se define como responsable del fichero a la «persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento». A la vista de este concepto, será necesario determinar quién, decide sobre la finalidad, objeto y uso de los datos.

A la vista de lo anterior, será cuestión fundamental resolver cuál es la finalidad a la que se encontrarían sujetos los ficheros que contuvieran los datos de los propietarios, tomando en consideración que la consulta plantea en todo caso la tenencia de dichos ficheros por el Administrador o Secretario.

En principio y así se desprendería del propio texto de la consulta la finalidad de mantener los datos de los propietarios es, precisamente, asegurar el cumplimiento por los propietarios de las obligaciones impuestas por la Ley de Propiedad Horizontal (en los términos previstos tras su reforma, operada por la Ley 8/1999, de 6 de abril), así como garantizar el adecuado ejercicio por los mismos de los derechos que les corresponden en la comunidad. En resumidas cuentas, la finalidad perseguida por el mantenimiento de estos ficheros será la de asegurar el correcto desenvolvimiento de la comunidad.

De lo antedicho se desprende que la condición de responsable del fichero recaerá sobre la propia Comunidad de Propietarios que es quien, a través de sus Órganos de Gobierno y, en su caso, de la Junta, resolverá sobre las cuestiones relacionadas con la misma, siendo así que, de lo establecido en el artículo 13 de la Ley se desprende que el Secretario y el Administrador, cuando actúen en el ejercicio de las funciones relacionadas con una determinada comunidad, no son sino órganos integrados en la misma, independientemente de la posibilidad de que una misma persona desempeñe funciones de secretario y/o administrador en varias Comunidades de propietarios. La misma solución se alcanza si se tiene en cuenta que le artículo 13.7 de la Ley, en su

párrafo segundo, habilita a la Junta a remover a quienes desempeñen funciones en uno de sus órganos de gobierno, siendo potestad de la Junta nombrar y separar a los mismos (artículo 14.1).

Las actividades que el Administrador (o, en su caso, el Secretario) de una determinada comunidad de propietarios desarrolle como tal no serán sino las derivadas de su propia integración, como órgano de gobierno, en la citada comunidad, sin que el mismo pueda utilizar la información de que tenga conocimiento como consecuencia del ejercicio de su función para un fin distinto del derivado de la gestión que le haya sido encomendada, en el ámbito de las funciones que al administrador atribuye el artículo 20 de la Ley de Propiedad Horizontal.

En consecuencia, la condición de responsable de los ficheros creados para la adecuada gestión y funcionamiento de la comunidad de propietarios de un inmueble objeto de división horizontal corresponderá a la propia Comunidad, que dispondrá a través de sus órganos de gobierno de toda la información facilitada por los propietarios, siendo el administrador, en cuanto tal y con relación a esa determinado Comunidad, un mero usuario del fichero, en virtud de su condición de órgano de gobierno de la comunidad.»

4.2.2. *Cesiones de datos*

— *Cesión de datos de un Ayuntamiento a la prensa*

Se planteó una consulta sobre si es legal que un responsable político municipal filtre a la prensa local datos sobre los supuestos pagos efectuados a un ciudadano como consecuencia de su colaboración con el Ayuntamiento. Dentro de la respuesta formulada por la Agencia, cabe extractar lo siguiente:

«Dos cuestiones son las que hay que destacar de su consulta, señalando, de un lado, la posibilidad de que un Concejal de la Corporación pueda tener acceso a la información personal que pueda estar contenida en los ficheros municipales, y de otro lado, si una vez obtenida esa información la puede ceder a terceros.

Con carácter general y respecto de la primera cuestión, el artículo 11.1 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) dispone que «los datos de carácter personal objeto de tratamiento solo 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»; esta disposición se ve complementada por lo dispuesto en el artículo 11.2 a), del que se desprende que será posible la cesión cuando una Ley lo permita.

La solicitud podría fundamentarse en la necesidad de que los Concejales solicitantes estén debidamente informados, a fin de llevar a cabo su función de control sobre la actividad del equipo de Gobierno del Ayuntamiento, en los términos previstos en el artículo 77 de la Ley 7/1985, de 2 de abril de Bases de Régimen Local. Este artículo prevé que: «todos los miembros de la Corporaciones locales tienen derecho a obtener del Alcalde o Presidente 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.

Teniendo en cuenta 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, el acceso a estos datos se encuentra amparada en los artículos 11.2 a) y 21. 1 de la LOPD.

Por lo que se refiere a la segunda cuestión, hay que señalar que los cesionarios (concejales) sólo podrán utilizar los datos en el ámbito de sus competencias, toda vez que éste es el límite establecido en la Ley de Bases de Régimen local, indicando a su vez que el artículo 4.2 de la LOPD establece que los datos no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Por este motivo, se indicó que, en caso de que pudiese acreditarse que la información publicada provenía del responsable político municipal, la cesión podría resultar contraria a lo establecido en la LOPD, informándose al interesado del modo en que podría, en su caso, denunciar los hechos ante la Agencia de Protección de Datos.

— ***Publicación en el Boletín Oficial de la Región de Murcia de una lista de afectados por un procedimiento de expropiación forzosa***

Se pregunta si dicha publicación resulta conforme con lo establecido en la LOPD. Se respondió que la publicación es lícita desde el punto de vista de la protección de datos, razonándose esta conclusión del siguiente modo:

«La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal establece que los datos personales no podrán ser comunicados a terceros salvo que se tenga el consentimiento de los afectados o que la cesión venga prevista en una ley.

En el caso planteado es la propia Ley de Expropiación Forzosa y su Reglamento de desarrollo, los que establecen el procedimiento a seguir en la tramitación de los expedientes de expropiación que se realicen por la Administración Pública.

Dicho procedimiento está sometido por la ley al principio de publicidad y en virtud del mismo, se establece legalmente la obligación de publicar la relación de los datos personales de los afectados por dicho expediente (nombre y domicilio, finca objeto de expropiación, etc.) en el Boletín Oficial del Estado, de la Provincia, o de las Comunidades Autónomas, así como en algún periódico de ámbito provincial, precisamente con el objeto legal, de dar a conocer públicamente el procedimiento de expropiación y permitir a cualquier interesado en el mismo que pueda realizar alegaciones.»

— ***Comunicación de datos a través de una página Web***

Se planteó consulta por un ciudadano al que le interesa conocer si la introducción de sus datos personales en una página *Web* del Colegio donde trabaja necesita de su consentimiento. En contestación a esta consulta se le indicó lo siguiente:

»La difusión por Internet de los datos de carácter personal es criterio de esta Agencia que constituye una cesión de datos, definida por el artículo 3 i) de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal como « toda revelación de datos realizada a una persona distinta del interesado».

En relación con las cesiones, el artículo 11.1 de la propia Ley 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». Esta regla general de consentimiento sólo se verá exceptuada en los supuestos contemplados en el artículo 11.2 de la ley, entre los que no tendría cabida el sometido a consulta.

En consecuencia, será necesario recabar, con carácter previo a la publicación, el consentimiento de los afectados para poder efectuar dicha divulgación, consentimiento que deberá ir precedido de la información sobre la finalidad a que se destinaran los datos o la actividad del cesionario.»

— ***Comunicación de datos a los socios de una Sociedad de Responsabilidad Limitada***

Se planteó la conformidad con la legislación de protección de datos de la posibilidad de acceso por los socios de una sociedad de responsabilidad limitada a la información de las cuentas anuales de la sociedad y de las nóminas de los trabajadores o administradores de la misma. Al respecto, se indicó lo siguiente:

«Con carácter general el apartado 1 de articulo 11 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal dispone que: los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un terceros para el cumplimiento de los fines directamente relacionados con las funciones legitimas del cedente y del cesionario con le previo consentimiento de interesado». Esta disposición de carácter general tiene una serie de excepciones previstas en el apartado 2, entre las que se encuentra la excepción legal, y en este sentido si una ley prevé la posibilidad de la cesión, no será necesario el consentimiento del afectado para que la misma pueda llevarse a efecto. Habrá que analizar, por tanto si existe norma legal que habilite y permita la cesión en el caso concreto planteado. En este sentido y tal y como se señala en el escrito de consulta, el artículo 86 de la Ley 2/1995 de Sociedades de Responsabilidad Limitada regula el ejercicio del derecho de examen de la contabilidad estableciendo que:

1. *A partir de la convocatoria de la Junta General, cualquier socio podrá obtener de la sociedad, de forma inmediata y gratuita, los documentos que han de ser sometidos a la aprobación de la misma, así como el informe de gestión y, en su caso, el informe de los auditores de cuentas. En la convocatoria se hará mención de este derecho.*

2. *Durante el mismo plazo y salvo disposición contraria de los estatutos, el socio o socios que representen al menos el 5 por 100 del capital podrán examinar en el domicilio social, por si o en unión de experto contable, los documentos que sirvan de soporte y de antecedentes de las cuentas anuales.»*

Sobre la base de la previsión legal anterior y en relación con la excepción del artículo 11.2 a) de la LOPD, parece que, en principio, el socio podrá analizar toda la documentación que sirva de soporte para la elaboración de las cuentas anuales, información que contendrá todas las cuentas globales de ingresos y gastos y demás documentos contables que se le presenten con el objeto de su aprobación.»

4.2.3. *Datos especialmente protegidos*

— *Comunicación al empresario de los datos de salud de los trabajadores y tratamiento de los mismos por aquél*

Se planteó una consulta referida a la posibilidad de que por un determinado Ayuntamiento se procediera a la digitalización de las historias clínicas de sus empleados, facilitadas por los servicios médicos del mismo. La Agencia contestó a la consulta en los siguientes términos:

«El artículo 22 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales establece que el empresario garantizará a los trabajadores a su servicio la vigilan-

cia periódica de su estado de salud en función de los riesgos inherentes al trabajo, siempre que el trabajador preste su consentimiento, salvo que dicho reconocimiento sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores.

No obstante lo anterior, la misma norma prevé que dicho reconocimiento se realizará respetando el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud, estableciendo en este sentido que el acceso a la información medica de carácter personal se limitará al personal médico y autoridades sanitarias que lleven a cabo la vigilancia de la salud, sin que pueda facilitarse dicha información al empresario o a otras personas, sin consentimiento expreso del trabajador.

En consecuencia y a la vista de la regulación anterior se le informa que, si el trabajador no consiente expresamente que sus datos personales de salud sean facilitados al empresario, éste sólo podrá ser informado de las conclusiones que se deriven de los reconocimientos en relación con la aptitud del trabajador para el desempeño de su puesto, pero en ningún caso estará habilitado para el tratamiento informático de ningún dato de salud que no se refiera a dichas conclusiones.»

— *Derecho de acceso a informes médicos en expedientes judiciales y tiempo de conservación de los datos de historias clínicas*

Consulta por la que un ciudadano quiere conocer diferentes aspectos del derecho de acceso a los informes médicos que pueden constar en los expedientes judiciales, así como la obligación que tienen las clínicas y hospitales públicos de conservar los datos de salud de los pacientes.

«Se le indica que toda la información concerniente a personas físicas que se encuentre en expedientes judiciales estará dentro del ámbito de aplicación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, si bien dichos expedientes al no estar informatizados tienen un periodo de adaptación a la LOPD que termina en el año 2007, aunque los derechos de acceso rectificación y cancelación deberán ser atendidos, de conformidad con lo previsto en la disposición adicional de la referida Ley orgánica.

No obstante lo anterior también se le indica que la forma de acceder a esta información se hará en los términos y previsiones legales contenidos en los artículos 234 y 235 de la Ley Orgánica 6/1985 del Poder Judicial.

El artículo 234 establece que los Secretarios y personal competente de los Juzgados y Tribunales facilitarán a los interesados cuanta información soliciten sobre el estado de

las actuaciones judiciales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas conforme a la ley. En los mismos casos, se expedirán los testimonios que se soliciten, con expresión de su destinatario, salvo en los casos en que la ley disponga otra cosa.

El artículo 235 establece que 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.

En segundo lugar y por lo que se refiere al tiempo en que se puede conservar los datos contenidos en una historia clínica, se le indica que la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal establece una regla general en su artículo 4.5, párrafo primero, que 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».

En particular, en lo relativo a las historias clínico-sanitarias, la norma de referencia es el artículo 61 de la Ley 14/1986, de 25 de abril, General de Sanidad, según el cual «en cada Area de Salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial. Estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Los poderes públicos adoptarán las medidas precisas para garantizar dichos derechos y deberes.»

Del juego de estas normas se desprende, por una parte, la necesidad de que los datos relacionados con la salud de los pacientes puedan ser adecuadamente conocidos por parte de los facultativos que, en su caso, pudieran tratar a los mismos y, por otra, la necesidad de que la conservación de la historia médica del paciente se produzca de tal modo y en tales condiciones que aseguren la confidencialidad de la información y garanticen la intimidad de los pacientes.

Ello supone, a nuestro juicio, que los datos contenidos en la historia clínica, en cuanto se relacionen con la salud del individuo y su consulta pueda resultar adecuada para preservar dicha salud, deberán conservarse, en principio, durante la vida del paciente, sin que pueda considerarse adecuada una cancelación de dichos datos que pudiera perjudicar la salud futura del paciente al que se refieren los datos médicos. Así se desprende del hecho de que la Ley imponga que el historial médico deberá estar «a dispo-

sición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo».

No obstante, es necesario indicar que la consulta fue respondida con anterioridad a la aprobación de la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo artículo 17 regula la conservación de la historia clínica, estableciendo el apartado 1 del mencionado artículo que *«Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.»*

Al propio tiempo, será necesario tener en cuenta lo establecido en la legislación autonómica en esta materia. Así, cabe hacer referencia a la Ley 21/2000, de 29 de diciembre de la Comunidad Autónoma de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica, la Ley 3/2001, de 28 de mayo, de la Comunidad Autónoma de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes o la Ley Foral de Navarra de 25 de abril de 2002, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica.

4.2.4. *Protección de datos en telecomunicaciones. Publicidad recibida por vía telefónica*

Se ha planteado una consulta referente a la realización de llamadas comerciales con mensaje grabado al número de teléfono de un ciudadano. En relación con dicho asunto, se indicó la normativa actualmente vigente, en los siguientes términos:

«En primer lugar debe indicarse que las llamadas no solicitadas para fines de venta directa están reguladas en el articulo 68 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 estableciendo lo siguiente:

«1. 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 (aparatos de llamada automática) o facsímil (fax), sólo podrán realizarse a aquellos que hayan dado su consentimiento previo.

2. Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas distintos de los establecidos en el apartado anterior, podrán

efectuarse salvo las dirigidas a aquellos que hayan manifestado su deseo de no recibir dichas llamadas.»

Por otra parte el articulo 67 de la referida norma establece en su apartado 2 que:

«Los abonados podrán exigir a los operadores que se les excluya de las guías, que se indique que sus datos personales no puedan utilizarse para fines de venta directa o que se omita parcialmente su dirección. Los operadores requeridos deberán cumplir lo dispuesto en este apartado, sin coste alguno para los abonados.

Los abonados que soliciten su exclusión de las guías, tendrán derecho a recibir la información adicional a la que se refiere el párrafo segundo del apartado 3 del artículo 69.»

A la vista de la normativa anterior, se indicó que la llamada efectuada al afectado podría ser contraria a las normas de protección de datos en caso de que la misma se realizase de forma automática y sin intervención humana, sin contar con su consentimiento, tal y como establece el artículo 68.1 citado.

En caso de que hubiera existido tal intervención humana, se indicó al afectado la conveniencia de que nuevamente se dirigiera por escrito a su operador, manifestándole su voluntad de que sus datos no figuren a ningún efecto en las guías telefónicas, o que los mismos no sean utilizados con fines comerciales, tal y como establece la legislación vigente.

4.2.5. *Deber de Secreto*

Se planteó una consulta sobre si una empresa puede facilitar información de una persona a otras de su propio entorno familiar. Se respondió en los siguientes términos:

«En contestación a esta consulta se informa que la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal regula en su artículo 10 el deber de secreto, de tal forma 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.

Basándose en dicho deber, cualquier entidad que maneje información personal, estará obligada a mantener en todo caso la confidencialidad de la misma y a no facilitar dicha información a nadie, con independencia de la relación que quien solicite la información guarde con el afectado al que los datos se refieren.

La vulneración del deber de secreto puede ser constitutiva de infracción leve en materia de protección de datos. Si la información revelada se refiriese a datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, la infracción será de carácter grave y, finalmente, si se revelase información que contuviera datos de ideología, religión, creencias, origen racial, salud o vida sexual así como datos recabados para fines policiales sin consentimiento de las personas afectadas, la infracción será de carácter muy grave.»

4.2.6. *Reglamento de Medidas de Seguridad*

— *Plazos de adaptación de las Medidas de Seguridad*

Se planteó una consulta referente a los plazos legalmente previstos para la implementación de las medidas de seguridad en los ficheros automatizados que contengan datos personales. En relación con la misma, se contestó lo siguiente:

«*El Real Decreto 994/1999, de 11 de junio, entró en vigor el 26 de junio de 1999. Su Disposición Transitoria Única prevé que «En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.*

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento».

Del mismo modo, debe recordarse que el Real Decreto 195/2000, de 11 febrero, amplió el plazo de aplicación de las medidas de nivel básico hasta el 26 de marzo de 2000. Al propio tiempo, por Resolución del Subsecretario de Justicia de 22 de junio de 2001, que publica el Acuerdo del Consejo de Ministros de la misma fecha, se amplió el plazo de implantación de las medidas de seguridad de nivel alto hasta el 26 de junio de 2002.

En consecuencia, las Medidas de Seguridad de nivel básico son exigibles desde el 26 de marzo de 2000, las de nivel medio desde el 26 de junio de 2000 y las de nivel alto desde el 26 de junio de 2002.

— *Auditorías: requisitos y plazos*

A continuación se reproduce la respuesta a una consulta referente a la figura del responsable de seguridad y a los requisitos y plazos aplicables a las Auditorías exigidas por el Reglamento de Medidas de Seguridad de ficheros automatizados:

«Se informa que la figura del responsable de seguridad se define en el artículo 2.11 del Real Decreto 994/99, donde únicamente se habla de persona o personas designadas por el responsable del fichero.

El responsable de seguridad no precisa de condiciones especiales, tan sólo las derivadas de un conocimiento técnico preciso de la materia y, en principio, puede ser el mismo responsable del fichero o persona designada libremente por éste.

La auditoría prevista en el artículo 17 para los sistemas de información, va referida para aquellos ficheros de datos que de conformidad con lo previsto en el artículo 4 deban adoptar las medidas de seguridad de nivel medio y alto, debiendo efectuarse cada dos años. Quedan exentos, por tanto, de esta obligación todos los ficheros de datos a los que solo se les exija las medidas de nivel básico.

Precisado lo anterior, se indica que no se puede informar sobre qué empresas pueden estar autorizadas para realizar dichas auditorías, dado que no existe ningún registro de las mismas, si bien cabe mencionar que existe una certificación, aunque no vinculante, que es la «certified information sistem auditor» (CISA), que se expide desde una asociación de Estados Unidos denominada «INFORMATION SISTEM AUDIT AND CONTROL ASSOCIATION» (ISACA). No obstante, no es exigible que los responsables de los ficheros acudan para la realización de las auditorías a profesionales que hayan obtenido esta certificación, dado que la misma no tiene carácter oficial.»

— *Nivel de seguridad aplicable al fichero de un videoclub que alquila películas pornográficas*

En contestación a esta consulta, se informó de lo establecido en el artículo 4 del Reglamento de Medidas de Seguridad.

De lo establecido en el mismo se desprende que si los ficheros incluyen valoraciones que permitan elaborar evaluaciones sobre la personalidad de las personas físicas, entonces el nivel de seguridad será medio. Si entre esas valoraciones se incluye información sobre ideología, religión, creencias, origen racial, salud o vida sexual, el nivel de protección será el alto. Si no concurre ninguno de los anteriores supuestos, el nivel de protección será el básico.

En el caso concreto, el mero hecho de alquilar películas pornográficas no presupone necesariamente el tratamiento de datos especialmente protegidos. No obstante, si el responsable del fichero incluyera valoraciones subjetivas sobre, por ejemplo, la orientación o vida sexual de los afectados, las medidas de seguridad a implementar habrían de ser las de nivel alto.

— *Documento de seguridad: contenido mínimo*

Planteada la cuestión sobre el contenido del documento de seguridad, se efectuó una breve descripción del mismo en los siguientes términos:

«El artículo 8 del Reglamento de Medidas de Seguridad recoge el contenido mínimo de los mismos, que será el siguiente:

1. *Ámbito de aplicación del documento.*
2. *Medidas, normas, procedimientos y estándares encaminados a garantizar el nivel de seguridad exigido.*
3. *Funciones y obligaciones del personal.*
4. *Estructura de los ficheros con datos personales y descripción de los sistemas de información que los tratan.*
5. *Procedimientos de notificación, gestión y respuesta ante las incidencias.*
6. *Procedimientos de realización de copias de respaldo y recuperación de los datos.*

Igualmente en dicho documento (artículo 9) deberán constar las funciones y obligaciones de las personas con acceso a los datos de carácter personal y a los sistemas de información que estarán claramente definidas y documentadas, debiendo adoptar el responsable del fichero 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.

El articulo 10 recoge lo que debe contener el procedimiento de notificación, gestión y respuesta ante las incidencias, estando definida una incidencia en el articulo 2 del mismo Reglamento.

El artículo 14 especifica el contenido de las copias de respaldo y recuperación, las cuales están igualmente definidas en el articulo 2.12.

Respecto al ámbito de aplicación del documento, se refiere al fichero o ficheros que están bajo el ámbito de aplicación del documento de seguridad (puesto que éste puede afectar a un solo fichero o a varios). Los recursos protegidos son las partes del sistema de información que quedan protegidos por el documento de seguridad.

Las normas y reglas encaminadas a garantizar el nivel de seguridad son las previsiones que el responsable del fichero tiene pensadas respecto al cumplimiento de las medidas de seguridad exigidas, es decir, cómo se van a llevar a cabo en la practica la adopción de las medidas que exige el Reglamento de seguridad.

Por último, la estructura de los ficheros y la descripción de los sistemas de información, se refiere a la composición interna de cada fichero incluido en el documento de seguridad (campos y registros incluidos en cada uno) así como la descripción del conjunto de ficheros, soportes y equipos empleados para el almacenamiento y tratamiento de los datos.»

— *Redes de Telecomunicaciones*

En relación con el Real Decreto 994/1999, que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, la consulta planteaba el ámbito de aplicación del artículo 26 del Reglamento que exige, dentro de las medidas de seguridad de nivel alto, el cifrado de los datos transmitidos a través de redes de telecomunicaciones o la utilización de mecanismos que garanticen que la información no sea inteligible ni manipulada por terceros. En relación con esta consulta, debe recordarse lo siguiente:

«*El artículo 26 sólo resultará de aplicación en aquellos supuestos que se refieran a la transmisión de datos incorporados a ficheros a los que hayan de ser aplicadas las medidas de nivel alto, delimitados en el artículo 4.3 del Reglamento que se refiere a «los ficheros que contenga datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas». En los demás supuestos, simplemente tendrá que tenerse en cuenta a lo dispuesto en el artículo 5 del Reglamento, a cuyo tenor: «las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local».*

En cuanto al ámbito de aplicación del articulo 26, debe estarse al hecho de que en la transmisión de los datos se empleen redes de telecomunicaciones, definidas por el artículo 2. c) de la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, e introducidos en la Ley 11/1998 General de Telecomunicaciones como «los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos mediante cable, o medios ópticos o de otra índole».

En consecuencia, las medidas a las que se refiere el artículo 26 del Reglamento serán de aplicación a la transmisión de datos entre distintas dependencias de la empresa cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa.

De acuerdo con dicha norma la obligación de cifrado de los datos corresponde al responsable que maneja y transmite dicha información utilizando redes de telecomunicaciones, debiendo utilizar procedimientos de cifrado que estén debidamente homologados por la Administración General de Estado de acuerdo con lo previsto en el articulo 52 de la Ley 11/1998, de24 de abril General de Telecomunicaciones.»

— *Nivel de protección de historias clínicas*

Se planteó por un ciudadano consulta referida al nivel de seguridad que deberá ser de aplicación a los ficheros en que se contienen los datos de las historias clínicas de pacientes. En contestación a la consulta se indicó lo siguiente:

«*La historia clínica es un documento donde se recoge y se contiene toda la información de utilidad médica relativa a la situación de salud o enfermedad de las personas, que tendrá como fin primordial el conocer de forma exacta, veraz y actualizada los datos médicos, para poder valorar por el personal sanitario el estado de salud de cada individuo concreto.*

En la medida en que la historia clínica contiene datos médicos, dicha información será calificada como datos de salud, y en consecuencia será una información que tendrá la consideración de especialmente protegida de conformidad con lo previsto en el artículo 7 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, siéndole de aplicación las medidas de nivel alto de protección de acuerdo con lo previsto en el artículo 4 del 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.

La responsabilidad sobre la historia clínica y sobre la aplicación de las medidas de seguridad recaerá sobre el responsable del centro medico que le atienda, donde se podrán ejercer los derechos de acceso, rectificación y cancelación en los términos contenidos en la LOPD (artículo 15 y siguientes).»

Nuevamente, debe recordarse lo que, respecto de las historias clínicas se establece en la Ley 41/2002, aprobada después de evacuarse la consulta transcrita.

Códigos Tipo

1. Introducción

El artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), prevé la posibilidad de formular códigos tipo a los responsables de ficheros, a través de acuerdos sectoriales o mediante decisiones de empresa o convenios administrativos, en los que se establezcan:

- 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.
- Garantías para el ejercicio de los derechos de las personas todo ello, con pleno respeto a los principios y disposiciones de la Ley y sus normas de desarrollo.
- Medidas a adoptar por el incumplimiento del código.

Este precepto de la LOPD corresponde a la trasposición del art. 27 de la Directiva, cuyo apartado 1 hace referencia a que «los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las peculiaridades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva». Por su parte, el apartado 2 del mismo precepto reitera esta configuración sectorial de los códigos tipo en la regulación comunitaria, al referirse únicamente a las «asociaciones profesionales» y a «las demás organizaciones representantes de otras categorías de responsables de tratamientos», como sujetos habilitados para adoptarlos.

Con el desarrollo de los códigos de conducta se pretende facilitar a las personas la posibilidad de ejercitar un control real de su esfera personal frente al avance de la tecnología, prevaleciendo el derecho fundamental a controlar y proteger su esfera privada.

Los códigos tipo tienen un papel fundamental para encontrar el equilibrio entre la aplicación de las nuevas tecnologías y el control de la privacidad, instrumentando la autorregulación a través de acuerdos y códigos privados, estándares de privacidad y sellos de garantía.

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

El objeto de la inscripción de los códigos tipo en el RGPD es el de darles publicidad, para ello, cualquier particular puede obtener una copia gratuita de ellos dirigiéndose al RGPD.
En esta materia la Agencia desea impulsar al máximo la elaboración de códigos tipo en aquellos sectores en los que puedan tener mayor relevancia, debido a factores tales como: singularidad del sector, sensibilidad de los datos tratados, población afectada, tecnologías utilizadas en el tratamiento de los datos, etc., en aras de facilitar el cumplimiento de la LOPD y ampliar las garantías ofrecidas al ciudadano en la protección de sus derechos. Para ello, la APD tiene como objetivo prioritario para los próximos años impulsar y colaborar en el desarrollo de nuevos códigos de conducta.

2. Códigos Tipo Tramitados en 2002

Durante 2002 se ha podido constatar en la Agencia un creciente interés en el desarrollo de nuevos códigos de conducta, y en este sentido, además de las actividades propias de la tramitación de los códigos tipo presentados se ha informado, tanto a través del teléfono como por escrito o mediante reuniones, a todas las personas que lo han solicitado.

De los códigos tipo tramitados en 2002, dos habían sido presentados en 2001, el Código Tipo de los profesionales del Colegio de Odontólogos y Estomatólogos de Cataluña y el 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 (APTICE).

Estos códigos no se inscribieron por no haberse aportado la documentación que acreditara representación suficiente, tanto del Colegio como de APTICE, por parte de las personas que presentaron las solicitudes.

Por otra parte, a lo largo de 2002, se presentaron otras cuatro solicitudes de códigos tipo. De nuevo, el Colegio de Odontólogos y Estomatólogos de Cataluña presentó un Proyecto de Código Tipo de los Profesionales de la Odontología y de la Estomatología de España. En este caso, también se denegó la inscripción al considerar que el Colegio de Cataluña no tiene competencia para extender el ámbito de aplicación del Código a todo el territorio español. En ambos casos, este código no se ha tramitado por no ajustarse a los requisitos formales

de presentación. Por otra parte, se han mantenido diversas reuniones con sus representantes para informarles de los aspectos que deben desarrollarse en un código.

La Asociación Catalana de Recursos Asistenciales (ACRA) presentó un proyecto denominado Código Tipo de ACRA, que no llegó a tramitarse debido a que con posterioridad se comunicó el desistimiento y por lo tanto no se llegó a tramitar su inscripción.

Para ambos proyectos, se han mantenido reuniones informativas con sus representantes y se ha puesto de manifiesto el interés demostrado por la elaboración de códigos tipo, por lo que es probable que en el ejercicio en curso puedan presentarse nuevos borradores que podrían dar lugar a la inscripción de los mismos.

El Código tipo de la Unión Catalana de Hospitales (UCH), y el Código ético sobre comercio electrónico y publicidad interactiva, de la Asociación Española de Comercio Electrónico (AECE), AUTOCONTROL e IAB Spain han sido los códigos presentados e inscritos durante 2002.

Por otra parte, junto con la inscripción de este último se produjo la supresión de las inscripciones del Código ético de comercio electrónico y marketing directo y el Código de Autocontrol de la Publicidad, ya que el nuevo código complementaba y sustituía a los anteriores.

Código Tipo de la Unión Catalana de Hospitales

El código de la UCH ha sido desarrollado con el objeto de definir una política de seguridad en el tratamiento de los datos personales de salud, dada su naturaleza de datos especialmente protegidos, y siendo conscientes de la conveniencia de establecer unas normas de conducta entre sus asociados que permitan la aplicación concreta de la legislación sobre protección de datos, como garantía para las personas afectadas por el tratamiento de sus datos. Para ello, se han establecido en el Código los criterios y condiciones que han de permitir la construcción de un corpus de buenas prácticas entre sus asociados, dirigidas directamente a garantizar, en el campo del tratamiento de datos concernientes a la salud de las personas afectadas, unos estándares de referencia en estricto cumplimiento de la Ley.

Dado el ámbito de especialización que diferencia a las organizaciones adheridas al Código, éste ha sido creado para convertirse en un documento ágil y eficaz, referencia para el sector sanitario, socio-sanitario y social, relativo a los datos de carácter personal, especialmente los concernientes a la salud de las personas, tratados en los denominados genéricamente ficheros de pacientes o historias clínicas.

Su principal objetivo es que los asociados al código tipo preserven la privacidad de las personas físicas y garanticen la autodeterminación informativa de los usuarios.

El código es de aplicación al tratamiento de datos de carácter personal contenidos en los ficheros de historias clínicas de los pacientes (en adelante, ficheros de pacientes), sea cual sea su soporte y modalidad de tratamiento, es decir, tanto ficheros informatizados o en soporte magnético, como ficheros convencionales no automatizados.

El código es fruto de un acuerdo de la Junta Directiva de la UCH de fecha 25 de abril de 2002, en la que se aprobó el texto del Código, refrendado por unanimidad en la Asamblea de asociados de la UCH de fecha 29 de abril de 2002.

La adhesión al código en ningún caso modifica el régimen de obligaciones establecido por la LOPD y resto de normativa legal vigente en materia de protección de datos. Por ello, los adheridos al código previamente cumplirán todas las obligaciones legales establecidas, con especial consideración las que se refieren a la notificación al RGPD de los ficheros existentes y la aplicación de las medidas de seguridad correspondientes, según el Reglamento de Seguridad.

El código garantiza la aplicación de los principios de protección de los datos contenidos en los ficheros de pacientes en los términos establecidos por la LOPD, así como las obligaciones del responsable en relación con los derechos de los afectados.

Nunca se tratarán datos con finalidades incompatibles a las que motivaron su recogida, aunque no es incompatible la finalidad posterior de carácter científico y/o histórico, siempre que los datos utilizados sean anónimos. Si se utilizasen datos para la realización de ensayos clínicos o proyectos de investigación, los correspondientes protocolos deberán prever mecanismos que permitan la disociación de los mismos con respecto a la identidad de los titulares. En todo caso, se incorporará la siguiente cláusula en los contratos entre el centro y el promotor del ensayo clínico:

«*El promotor del presente ensayo clínico garantiza que el protocolo del mismo establece los mecanismos que permiten la disociación de los datos de carácter personal contenidos en el fichero de pacientes en relación a los sujetos que participan en el ensayo. En cualquier caso se obliga el promotor a cumplir y hacer cumplir las prescripciones establecidas en la Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal en todo lo que haga referencia a los datos de dicha índole que sean utilizados en el desarrollo del ensayo.*»

El deber de información en la recogida de los datos al que hace referencia el art. 5 de la LOPD se formalizará mediante un documento informativo en el que se indica:

- Identificación del responsable del fichero y su domicilio.
- El nombre el fichero o tratamiento al que se destinan los datos recabados.
- Se informa de que la única finalidad del fichero es la del tratamiento médico sanitario.
- Destinatario/s de la información incluyendo, en su caso, la entidad concertada para la prestación de servicios médico-sanitarios del afectado, a efectos del pago de los costes correspondientes a la prestación recibida.

Se informa de la posibilidad de ejercitar los derechos de oposición, acceso, rectificación y cancelación reconocidos por la LOPD. El responsable del fichero cuidará de que se faciliten a los interesados el ejercicio de estos derechos mediante los modelos de solicitudes correspondientes, que se adjuntan al código tipo y que se entregarán al interesado con constancia de su recepción.

Cada entidad adherida es responsable de acreditar el cumplimiento de la obligación de informar, utilizando cualquier medio jurídicamente hábil a tal fin, entendiendo acreditado el cumplimiento mediante la custodia de un ejemplar del documento de información firmado por el usuario.

También se informará mediante la ubicación de paneles informativos en las áreas de admisiones y salas de espera de los centros.

Se garantiza la aplicación de medidas de seguridad organizativas y técnicas calificadas de nivel alto en el Reglamento de Seguridad para los ficheros automatizados de historias clínicas.

Por otra parte, como valor añadido, el código tipo presenta la obligación, por parte de las entidades adheridas, de adoptar una serie de medidas de seguridad, en relación con el uso y custodia de la historia clínica no automatizada para garantizar plenamente el derecho del paciente a su intimidad personal y el deber de guardar secreto para quien, en virtud de sus competencias, tenga acceso a la historia clínica.

Estos criterios serán incorporados al documento de seguridad de cada entidad adherida. En el caso de que, debidamente justificados, no pudieran ser implantados en la entidad, ésta establecerá medidas o criterios alternativos adecuados a las circunstancias de la entidad afectada.

Respecto a los ficheros de Historias Clínicas no automatizados, con el fin de garantizar unas medidas de seguridad adecuadas que permitan la protección de los derechos de los usuarios afectados, en tanto no se produzca un desarrollo reglamentario al respecto, el Código Tipo establece las fórmulas y mecanismos siguientes:

- Cada Historia Clínica ha de estar identificada por un número único para cada paciente de la entidad adherida y en ella se recogerá toda la información integrada y acumulativa relativa al curso clínico del paciente, incluyendo el acuse de recibo de que se ha facilitado al paciente la hoja de información en relación a sus derechos sobre los datos personales contenidos en la historia.

- Las Historias Clínicas se custodiarán en un archivo único, que contará con medidas de seguridad física apropiadas, pudiendo constituirse un archivo pasivo diferenciado, en el que se ubicarán las historias correspondientes a pacientes sin contacto con el centro durante un determinado periodo.

- En el caso de que este archivo pasivo se encuentre fuera de las dependencias del centro y gestionado por una empresa externa, deberá ser formalizado por escrito un contrato que regule expresamente el deber de confidencialidad del depositario de las Historias Clínicas, así como también el resto de obligaciones como encargado del tratamiento.

- En cada centro se establece un responsable de archivo de HC, que deberá velar por el adecuado cumplimiento de los sistemas de archivo, control e información, que deberán ser adecuados a las características y dimensiones del centro.

- Se establecen normas de acceso al archivo físico de Historias Clínicas, y los movimientos efectuados sobre las historias se reflejarán en un libro de registro mediante la anotación del motivo que origina la petición, fecha de entrega y fecha de devolución de la historia, de forma que sea posible su seguimiento. Durante la salida de la historia deberán establecerse medidas de seguridad mínimas que permitan restringir el acceso a personas no autorizadas.

- En ningún caso se permitirá la salida de una historia clínica de las dependencias del centro durante el periodo en que se ha hecho una petición por motivos asistenciales, docentes o de investigación.

- Si se produjera una petición de HC por personal facultativo ajeno al centro por motivos docentes o de investigación, diferentes del propio proceso asistencial, deberá recabarse previa autorización expresa del paciente, siempre que los datos de la HC no puedan ser entregados en modo disociado.

- Deberán establecerse los circuitos oportunos que permitan al paciente, o su representante legal, ejercer el derecho de acceso a su propia HC. La petición de acceso a la HC deberá ser realizada por escrito y de manera que se acredite la identidad del solicitante.

- El paciente tendrá en cualquier caso acceso a la información que conste en su HC relativa a informes de alta, informes de urgencias, informes de pruebas diagnósticas y exploraciones complementarias, analíticas y similares. Siempre que el profesional no invoque reserva al respecto, podrán entregarse también hojas de curso clínico y documentos similares que contengan apreciaciones subjetivas de los profesionales que han participado en el tratamiento del paciente.

- En ningún caso se entregará documentación original de la HC, debiendo informarse de manera previa al solicitante, del coste que pudiera suponer la obtención de copias de la misma en los casos en que la obtención de la copia tenga un coste extraordinario por el soporte de la misma, ofreciendo si es posible, alternativas al respecto.

- En aquellos casos en que se reciba una solicitud o requerimiento de información clínica procedente de la Administración de Justicia, solicitando la remisión de una HC se recabará la autorización del responsable del centro y únicamente se enviará copia de la documentación en ella contenida. La remisión de la HC se acompañará de un escrito del responsable del centro en el cual se manifieste el deber de confidencialidad de los datos clínicos.

- Las HC únicamente serán canceladas una vez transcurrido el plazo previsto por la normativa vigente (Ley 21/2000 de la Generalitat de Cataluña).

Los profesionales que prestan servicios en las entidades adheridas están sometidos al deber de obligación o deber de secreto profesional en relación con los datos personales contenidos en los ficheros de pacientes, inherente a la condición de profesiones vinculados al proceso asistencial, impuesto por sus propias normas deontológicas. No obstante, los responsables de los ficheros o tratamientos adheridos al código se comprometen a recordar esta obligación a sus profesionales.

En relación con el personal no vinculado al proceso asistencial con acceso a los datos de los ficheros de pacientes, la entidad obtendrá la firma de un documento de compromiso relativo al cumplimiento del deber de secreto, que contendrá las advertencias pertinentes en relación con las consecuencias que implicaría su incumplimiento, tanto desde una perspectiva disciplinaria laboral, como del derecho de repetición que la entidad ostenta ante posibles sanciones o indemnizaciones económicas a las que tenga que hacer frente.

UCH consciente de que la asistencia sanitaria, socio-sanitaria y social rara vez se puede llevar a cabo tan solo con los dispositivos y mecanismos propios de entidad responsable del fichero, haciéndose preciso el uso de servicios intermedios sanitarios externos y la realización de técnicas diagnósticas y terapéuticas especializadas, establece en el código tipo las

condiciones en que las entidades adheridas al código pueden encargar la realización de tratamientos de datos con terceros.

Siempre que sea necesario comunicar datos a un tercero encargado del tratamiento que no constituya una cesión de datos, se establecerá un contrato o acuerdo por escrito en el que se haga constar:

- Los datos serán tratados de acuerdo a las instrucciones facilitadas por el responsable.

- Se determinarán específicamente las finalidades para las que el encargado realizará los tratamientos, no pudiendo aplicarlas a ninguna otra finalidad, ni comunicarlos a terceros.

- Se obligará al encargado del tratamiento a implementar las medidas de seguridad pertinentes atendida la naturaleza de los datos de los ficheros de pacientes.

- Se determinará el procedimiento de devolución o destrucción de la información una vez finalizada la prestación contractual o cumplida la obligación legal de conservarlas, en caso de existir.

Estas condiciones se establecerán asimismo cuando la prestación de servicios consista en la gestión documental y el almacenamiento de los ficheros de pacientes en archivos convencionales.

El cumplimiento de las obligaciones establecidas en el código tipo se efectuará por un Comité Directivo creado al efecto en UCH.

Este Comité habilitará mecanismos de asesoramiento a las entidades adheridas, que les permitan resolver dudas y consultas puntuales, y mecanismos de información y consulta para los usuarios y ciudadanos en general a través de la web de UCH.

UCH diseñará un logotipo como símbolo distintivo de las entidades adheridas al código tipo, que se insertará en sus páginas web y en los paneles informativos de los centros adheridos. Por último, este código también prevé la resolución de conflictos mediante un procedimiento de derecho de queja, que resolverá el Comité, y la aplicación de un régimen disciplinario, todo ello sin perjuicio de las posibles reclamaciones que pudieran presentarse en la Agencia de Protección de Datos.

Código Ético sobre Comercio Electrónico y Publicidad Interactiva

El Código ético sobre comercio electrónico y publicidad interactiva se presentó conjuntamente por las asociaciones AECE, AUTOCONTROL e IAB Spain.

Este Código está promovido por las entidades anteriormente citadas, a las que se han adherido otras asociaciones que desarrollan su actividad en el marco de las comunicaciones comerciales y los nuevos medios electrónicos de comunicación a distancia, y que son las siguientes: Federación Española de Comercio Electrónico y Marketing Directo (FECEMD), la Asociación de Agencias de Marketing Directo e Interactivo (AGEMDI), la Asociación Española de Anunciantes (ANUNCIANTES), la Asociación Española de Agencias de Publicidad (AEAP), la Federación Nacional de Empresas de Publicidad (FNEP), la Asociación de Centrales de Medios (ACM), la Asociación de Medios Publicitarios (AMPE) y la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC).

Además, pueden adherirse al mismo otras organizaciones representativas del sector que deseen participar en este sistema de autorregulación.

Por otra parte, este Código ha sido informado por el Ministerio de Ciencia y Tecnología y el Instituto Nacional de Consumo.

Las entidades promotoras y adheridas al Código Tipo desarrollan su actividad en el marco de las comunicaciones comerciales y los nuevos medios electrónicos de comunicación a distancia.

El desarrollo del código tiene por objeto aportar una solución a los problemas de regulación en este sector, que dada su naturaleza dinámica, y en permanente evolución, conlleva que las posibilidades de obsolescencia normativa sean mayores que en cualquier otro, permitiéndole adaptarse a los cambios.

Asimismo, trata de resolver los interrogantes planteados ante los problemas de aplicación de la regulación legal existente, ante el imprevisible fenómeno planteado por el uso cada vez más amplio de lo que se ha dado en conocer como «nuevas tecnologías», y especialmente Internet.

En los años 1998 y 1999 se habían desarrollado al amparo de la derogada LORTAD e inscrito en el RGPD el Código Ético de Protección de Datos Personales en Internet, y el Código Ético sobre Publicidad en Internet, por AECE y AUTOCONTROL, respectivamente, contando cada uno de ellos con sus propios mecanismos de aplicación.

Por una parte, se hacía necesaria la adaptación de los citados Códigos a la actual LOPD, y por otra, a los avances tecnológicos y legales producidos desde su adopción, tales como la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de la Unión Europea, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva de Comercio Electrónico) y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

En este interés, AECE y AUTOCONTROL, decidieron aunar esfuerzos para establecer un sistema de autorregulación integral en el sector, que favorezca tanto a los consumidores como a la industria y la sociedad en general, que además, evite la confusión que podría producir la aparición de diferentes sistemas de autorregulación, que sustituya a los Códigos existentes con anterioridad. Además, a esta iniciativa se une el IAB Spain.

Todas las asociaciones participantes, en reunión conjunta celebrada al efecto en Madrid, el día 28 de octubre de 2002, se comprometieron a promover este Código Tipo entre sus miembros y a darlo a conocer y difundirlo tanto en los distintos sectores empresariales relacionados como en la sociedad española en general, especialmente entre los usuarios de Internet.

El Código establece un conjunto de normas deontológicas, en dos grandes áreas de regulación, como son las comunicaciones comerciales o publicidad y el comercio electrónico, realizados a través de medios electrónicos de comunicación a distancia, por personas físicas o jurídicas con establecimiento permanente en España o dirigidos de forma específica al mercado español.

El Código considera medios electrónicos de comunicación a distancia y publicidad los determinados por la LSSI.

No se considera publicidad o comunicación comercial, a los efectos del código, los datos que permiten acceder directamente a la actividad de una empresa, organización o persona, y concretamente el nombre de dominio o la dirección de correo electrónico, en los mismos términos establecidos en la definición de Comunicación comercial de la LSSI.

Sin embargo, los datos de carácter personal, quedan definidos a los efectos del Código como «cualquier información concerniente a personas físicas identificadas o identificables, y entre otros, la dirección personal de correo electrónico y el número de teléfono, siempre que permitan identificar a su titular».

Se establecen principios y reglas de conducta generales, que resultan exigibles a los operadores en sus transacciones con los consumidores para la contratación de bienes y servicios

a través de medios electrónicos de comunicación a distancia, con el fin de dar adecuada respuesta a la necesidad de mantener altos niveles de protección de sus derechos e intereses, resaltando las áreas de protección de datos personales y protección de los menores.

Respecto de la protección de datos personales, el texto del Código articula en el Título IV —Protección de Datos Personales— las previsiones sobre la materia.

En este Título se establecen los principios y garantías adicionales a la LOPD, que van a ofrecer las entidades adheridas al sistema.

A continuación se recogen las consideraciones de especial relevancia del Código a este respecto.

En la recogida de datos a través de medios electrónicos de comunicación a distancia, además de la cláusula informativa prevista en el art. 5 de la LOPD, las empresas adheridas a este Código van a ampliar esta información con la inclusión del código o número de inscripción del fichero en el RGPD. Asimismo, van a facilitar los datos de identificación del responsable del tratamiento de los datos, junto con la dirección postal y la dirección de correo electrónico para facilitar la comunicación.

En relación con esta información, a los efectos de este Código y en cumplimiento de la LSSI, cualquier empresa que realice comunicaciones comerciales a través de medios electrónicos de comunicación a distancia, facilitará de forma clara, directa y fácilmente accesible, su nombre o denominación social, su domicilio a efectos legales así como su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

Las empresas que se anuncian en Internet y que recaban, capturan y tratan datos personales, informarán a los consumidores, mediante un aviso en su *web*, de dicho tratamiento. De tal forma que el consumidor, puede, si lo desea, ejercitar su derecho de oposición tanto en lo que se refiere a la captación de los datos, como a su tratamiento y posible transferencia.

Para garantizar a los titulares de los datos el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, las empresas adheridas ponen a su disposición mecanismos de utilización sencillos, como la dirección de correo postal.

Las empresas adheridas al sistema proveerán a los usuarios de información clara y comprensible sobre la presencia y la finalidad de las *«cookies»* y otros dispositivos o técnicas similares, poniendo a su disposición mecanismos sencillos y gratuitos para informarles sobre cómo desactivarlas. Asimismo, se avisará de forma clara cuándo queda imposibilita-

do el acceso o la utilización de un servicio interactivo por ser necesario el envío e instalación de *«cookies»* y otros dispositivos o técnicas similares en el terminal del usuario.

En el caso de emplearse *«cookies»* u otras técnicas, se utilizarán de forma disociada y nunca individualizada o relacionada a los datos personales de los usuarios, de forma que la información que se obtenga no pueda asociarse a persona identificada o identificable, salvo que el consumidor haya dado su consentimiento. En el caso de utilizar *«cookies»* o *«pixels»* transparentes u otras técnicas asimilables, se proporcionará a los usuarios información clara y comprensible sobre su objetivo y de su utilización desvinculada de cualquier dato de carácter personal.

Estas condiciones para el tratamiento de las *«cookies»* es extrapolable por analogía a otras técnicas de monitorización de la conducta de los usuarios en su utilización de medios electrónicos de comunicación a distancia.

Las empresas adheridas al Código se comprometen a no utilizar grupos de noticias, tablón de anuncios o foros o charlas para captar datos con finalidad publicitaria, salvo que dicha recogida se ajuste a las normas de obtención de datos establecidas en el presente Código.

También deberán respetar la privacidad de los usuarios, así como asegurar el secreto y seguridad de los datos personales, adoptando para ello las medidas técnicas y organizativas necesarias.

Por último, las empresas adheridas a este Código deberán apoyar iniciativas para ayudar a educar al consumidor sobre cómo proteger su intimidad en los medios electrónicos de comunicación a distancia.

El Código establece un sistema de aplicación de las reglas para resolver bajo los principios de independencia, transparencia, contradicción de las partes, eficacia, legalidad, libertad y representación, las controversias y reclamaciones que se presenten por eventuales incumplimientos de las reglas o normas del Código Tipo. Este sistema se basa en la actividad del Jurado de la Publicidad, dependiente de AUTOCONTROL, a través de un Convenio suscrito con el Instituto Nacional de Consumo, para todas las cuestiones relacionadas con las comunicaciones comerciales, y la Junta Arbitral Nacional de Consumo, para las cuestiones de carácter contractual con los consumidores que se puedan suscitar, previo intento de mediación por parte de AECE. Esta Junta encomienda a un Colegio Arbitral la resolución de las controversias, con el sometimiento voluntario de las dos partes en conflicto, y sus pronunciamientos tienen la eficacia de un laudo arbitral.

Todo ello, sobre la base de lo previsto en los artículos 16 «Códigos de conducta» y 17 «Solución Extrajudicial de litigios» de la Directiva de Comercio Electrónico y la LSSI, y sin perjui-

cio de las actuaciones que pudieran efectuarse desde la Agencia de Protección de Datos como consecuencia del incumplimiento de la LOPD.

Además, el Código establece una Secretaría que asegurará la adecuada coordinación y eficacia en la tramitación de las reclamaciones que se reciban, impulsando y coordinando el procedimiento ante estos órganos.

Por último, el sistema de autorregulación lleva asociado un sello de confianza que permite identificar las empresas y compañías adheridas al mismo.

La Protección de Datos en España.
Análisis de los principales desarrollos

1. Informes sobre Proyectos de Disposiciones Generales

De conformidad con lo establecido en el artículo 37 h) de la LOPD corresponde a la Agencia de Protección de Datos informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica. Por su parte, el artículo 5 del Estatuto de la Agencia concreta, en sus apartados a) y b), este precepto, estableciendo que la Agencia informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica, así como cualesquiera proyectos de ley o reglamentos que incidan en la materia propia de la Ley Orgánica.

A lo largo de 2002 se han sometido al parecer de la Agencia de Protección de Datos, para su informe preceptivo, un total de 33 disposiciones, debiendo destacarse por su especial relevancia las siguientes:

- Anteproyecto de Ley de Estadística de Castilla-La Mancha.

- Anteproyecto de Ley de Firma Electrónica.

- *Proyecto de Ley de la Agencia Catalana de Protección de Datos.*

- Proyecto de Ley de Prevención y bloqueo de la financiación del terrorismo.

- Borrador de Anteproyecto de Ley por la que se regulan los ficheros de datos de carácter personal de titularidad pública y se crea la Agencia Vasca de Protección de Datos.

- Enmienda al Proyecto de Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, relativa a la retención de datos de tráfico por parte de los operadores de telecomunicaciones y los proveedores de acceso a Internet.

- Proyecto de Orden Ministerial reguladora de los ficheros automatizados de datos de carácter personal gestionados por el Ministerio de Agricultura, Pesca y Alimentación.

- Proyecto de Real Decreto por el que se establece la garantía al ciudadano del tiempo de acceso a las prestaciones del Sistema Nacional de Salud.

- Proyecto de Real Decreto por el que se aprueba el Reglamento General del Mutualismo Administrativo.

- Proyecto de Real Decreto para el impulso de la Administración electrónica.

- Proyecto de Reglamento de la Ley Orgánica 5/2000, reguladora de la responsabilidad penal de los menores.

- Proyecto de Real Decreto por el que se aprueba el Reglamento del Registro General de la Propiedad Intelectual.

- Proyecto de Real Decreto por el que se establecen los procedimientos y las medidas técnicas para la interceptación legal de las telecomunicaciones exigibles a los operadores de servicios de telecomunicaciones disponibles al público y de redes públicas de telecomunicaciones.

- Proyecto de Orden sobre regulación de los ficheros de datos de carácter personal del Ministerio de Educación y Cultura.

- Proyecto de Orden Ministerial reguladora de los ficheros automatizados de datos de carácter personal gestionados por el Ministerio de Fomento.

- Proyecto de Orden por el que se incorporan ficheros a la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento.

- Proyecto de Orden Ministerial por la que se determinan los ficheros automatizados con datos de carácter personal del Ministerio de Justicia y de sus organismos.

- Proyecto de Orden por la que se regulan los ficheros automatizados de datos de carácter personal del Ministerio de Medio Ambiente.

- Proyecto de Orden por el que se amplía la de 21 de julio de 1994, que regula los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo.

- Proyecto de Orden del Ministerio del Interior por la que se regulan los ficheros informáticos de la Dirección General de la Policía.

- Propuesta de Orden Ministerial por la que se regulan los ficheros automatizados de datos de carácter personal correspondiente al Cuerpo de Notarios.

- Propuesta de Orden del Consejero de Interior del Gobierno Vasco, reguladora de los ficheros automatizados de datos de carácter personal del Departamento de Interior y del Organismo Autónomo «Academia de Policía del País Vasco» adscrito al mismo.

Debe indicarse que entre los proyectos de disposiciones generales informadas en el periodo comentado, ha sido especialmente significativo el número de 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 Protección de Datos.

2. Consultas de Responsables de Ficheros

El Gabinete Jurídico, incardinado en la Unidad de Apoyo al Director de la Agencia, ha venido ejerciendo, desde la creación de la Agencia de Protección de Datos, y junto con la función consultiva y de asesoramiento en Derecho a los distintos órganos de la propia Agencia que le es propia, 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 2002 se ha mantenido el importante volumen de actividad desplegado en el ejercicio de esta función, que desarrolla la Agencia aún 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 415 informes. Aunque el número de los mismos ha descendido ligeramente respecto de los que se emitieron en el año 2001, debe destacarse cómo se ha incrementado notablemente, en muchos casos, la complejidad de las cuestiones planteadas, descendiendo correlativamente el volumen de consultas que han sometido cuestiones más simples o reiteradas otros años.

De este modo, cuestiones planteadas de modo reiterado en años anteriores han descendido en gran número, habida cuenta la importante labor divulgativa efectuada durante esos ejer-

cicios anteriores que ha permitido conocer en profundidad dichas materias, reduciendo el número de consultas relacionadas con las mismas. A título de ejemplo, las cuestiones relacionadas con el tratamiento y cesión de los datos del Padrón Municipal han descendido ininterrumpidamente desde las casi 100 planteadas en 1999 a las 35 formuladas en 2002.

Por contra, en 2002, se ha contabilizado un importante volumen de consultas relacionadas con la publicación y la cesión de datos de carácter personal en Internet y con las actividades relacionadas con la prestación de servicios de la sociedad de la información y los operadores de telecomunicaciones, lo que pone de manifiesto la importancia cada vez mayor de este sector, tanto en el ámbito público como en el privado.

Asimismo, debe destacarse el notable incremento de las cuestiones relacionadas con las características y formas de prestación del consentimiento para el tratamiento de los datos de carácter personal, poniendo este hecho de manifiesto la cada vez mayor problemática relacionada con esta figura.

Del mismo modo, se han incrementado notablemente las cuestiones relacionadas con las comunicaciones de datos a las Administraciones Tributarias (que casi se han triplicado durante el ejercicio) y las relacionadas con el sector policial.

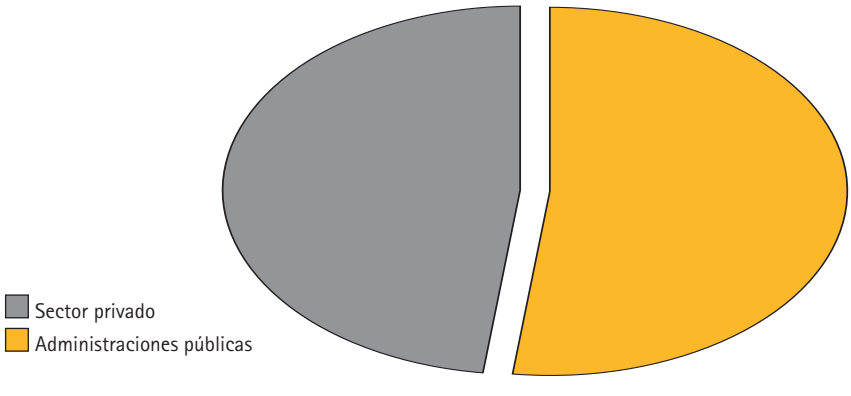
Igualmente, ha sido importante el volumen de cuestiones referidas al criterio de la Agencia de Protección de Datos en relación con las transferencias internacionales, dentro de una práctica creciente de transmisiones de datos por parte de empresas españolas a sus filiales o matrices en el extranjero, 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.

2.1. 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	**199**
Administración General del Estado	82
Comunidades Autónomas	27
Entidades Locales	66
Otros organismos públicos	24
Consultas Privadas	**216**
Empresas	167
Particulares	13
Asociaciones/Fundaciones	20
Sindicatos	4
Otros	12
Total informes	**415**

CONSULTAS PRIVADAS-PÚBLICAS



Como puede observarse, del volumen de informes evacuados a instancia de responsables de ficheros durante el año 2002, 208 han correspondido a consultas privadas, mientras que 199 han sido las planteadas por las Administraciones Públicas, pudiendo reseñarse que en este año ha seguido siendo mayor (al igual que ocurrió en años anteriores) el número de consultas planteadas por particulares (personas físicas o jurídicas), aunque también debe ponerse de manifiesto que, siguiendo la tendencia iniciada durante 2001, ha aumentado

proporcionalmente el número de las remitidas por las Administraciones Públicas, que se acercan paulatinamente a la mitad del total.

Considerando estas cifras, puede apreciarse cómo, respecto a las cuestiones planteadas por el sector público, ha disminuido respecto al año anterior el número de las consultas formuladas por Ayuntamientos, que incluso pasan a ser menores en número a las remitidas por la Administración General del Estado que, por el contrario aumentan en torno a un 20 por 100. Del mismo modo, las consultas planteadas por las Administraciones Autonómicas aumentan en casi un 70 por 100, descendiendo en similar proporción las provenientes de la Administración corporativa, lo que puede deberse a las actuaciones desarrolladas por la Agencia en estrecha colaboración con los Colegios Profesionales y las Cámaras de Comercio, Industria y Navegación dentro del marco de los distintos protocolos de colaboración celebrados con estas entidades.

Por su parte, en cuanto a las consultas del sector privado, y al igual que ha venido sucediendo en años anteriores, predominan notablemente las consultas planteadas por empresarios.

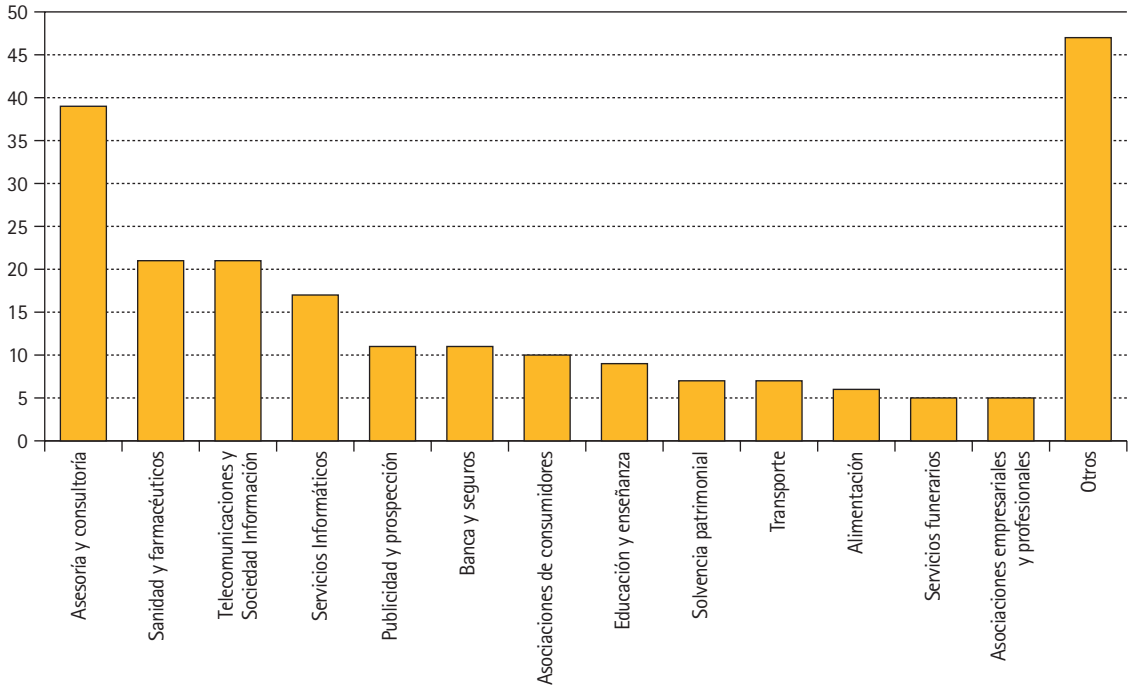
Atendiendo a la distribución sectorial de las consultas, cabe destacar la notoria reducción de las planteadas por entidades que realizan actividades de asesoría y consultoría (que descienden en un 75 por 100 en los dos últimos años). Esta reducción se debe al hecho de que las consultas planteadas se han centrado en las relativas a la gestión de los propios ficheros de estas entidades, dado que, como se ha indicado en anteriores Memorias, se ha dejado constancia a las mismas que, en lo referente a las cuestiones planteadas en relación con la función asesora de los clientes responsables de ficheros, se estaría obligando a la Agencia de Protección de Datos (al margen de las previsiones de la Ley Orgánica y del Estatuto) a llevar a cabo actividades propias de dichas entidades, entrando en concurrencia con éstas.

Por otra parte, debe destacarse el notable incremento de las consultas planteadas por el sector sanitario y el de telecomunicaciones (que doblan las cifras correspondientes a 2001), así como las entidades prestadoras de servicios informáticos. En relación con el sector de las telecomunicaciones, las cifras referidas al sector privado deben complementarse con las 11 consultas formuladas por la Comisión del Mercado de las Telecomunicaciones, si bien sus datos se encuentran recogidos, lógicamente, dentro de las cifras referidas al sector público.

También resulta relevante, por novedoso, el volumen de las consultas formuladas por las asociaciones de consumidores y usuarios, las empresas de transporte y alimentación, así como las prestadoras de servicios funerarios.

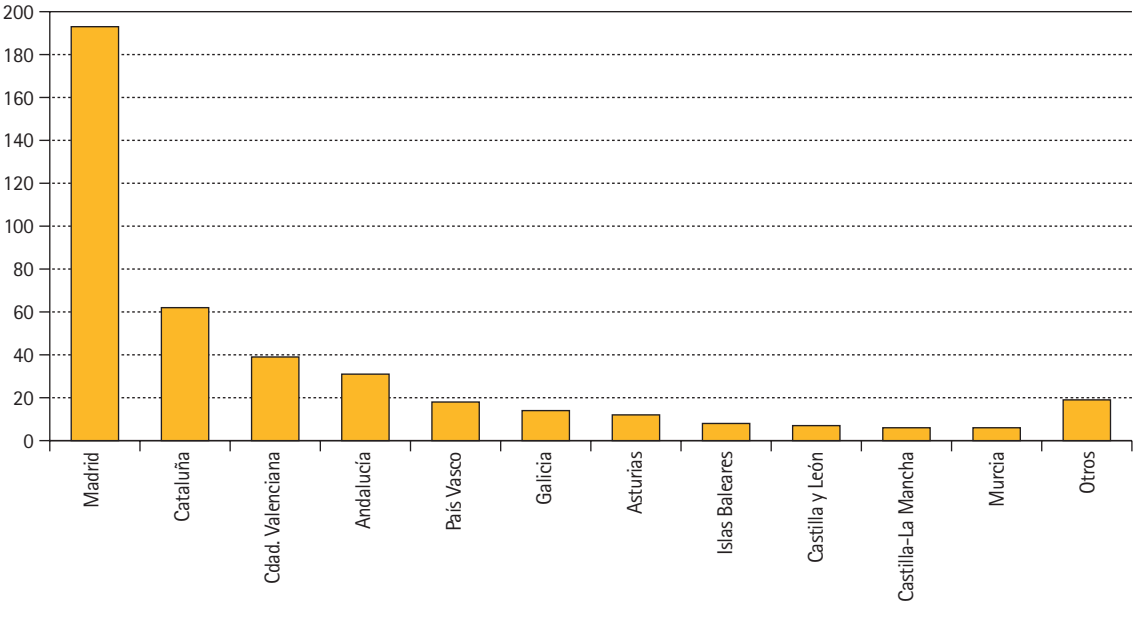
En relación con las cuestiones que acaban de exponerse, puede establecerse la siguiente distribución por sectores de actividad:

CONSULTAS POR SECTORES DE ACTIVIDAD

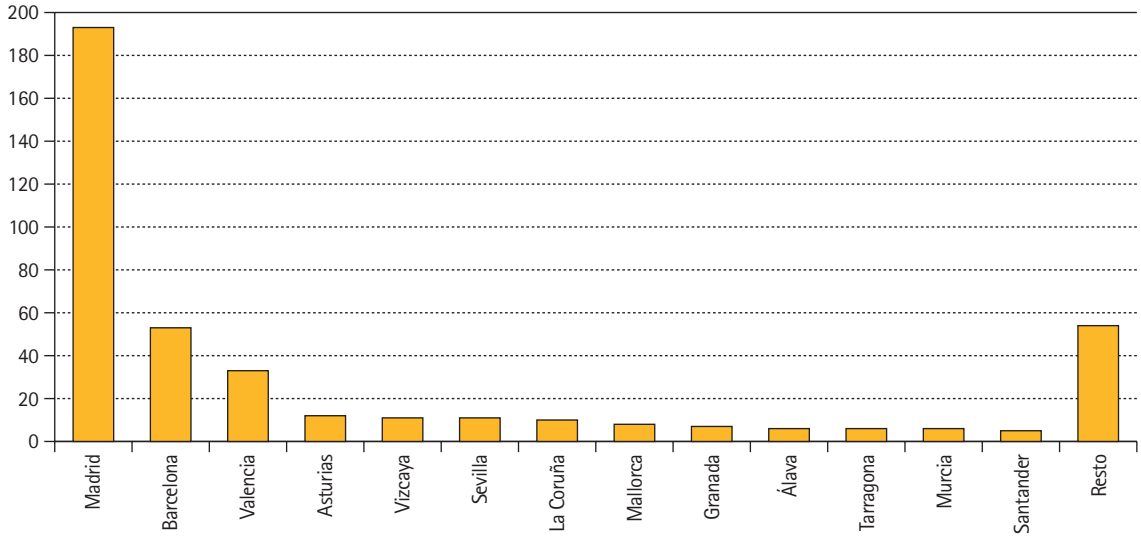


También ha existido una continuidad respecto al pasado año en cuanto a la distribución geográfica de las consultas planteadas, cuya distribución se ofrece a continuación, tanto por Comunidades Autónomas como por provincias. Como puede comprobarse, y siguiendo la tendencia de años anteriores, las consultas formuladas por personas y entidades ubicadas en la Comunidad de Madrid alcanzan prácticamente la mitad del total, seguidas a mucha distancia por Cataluña y la Comunidad Valenciana.

DISTRIBUCIÓN POR COMUNIDADES AUTÓNOMAS



DISTRIBUCIÓN POR PROVINCIAS

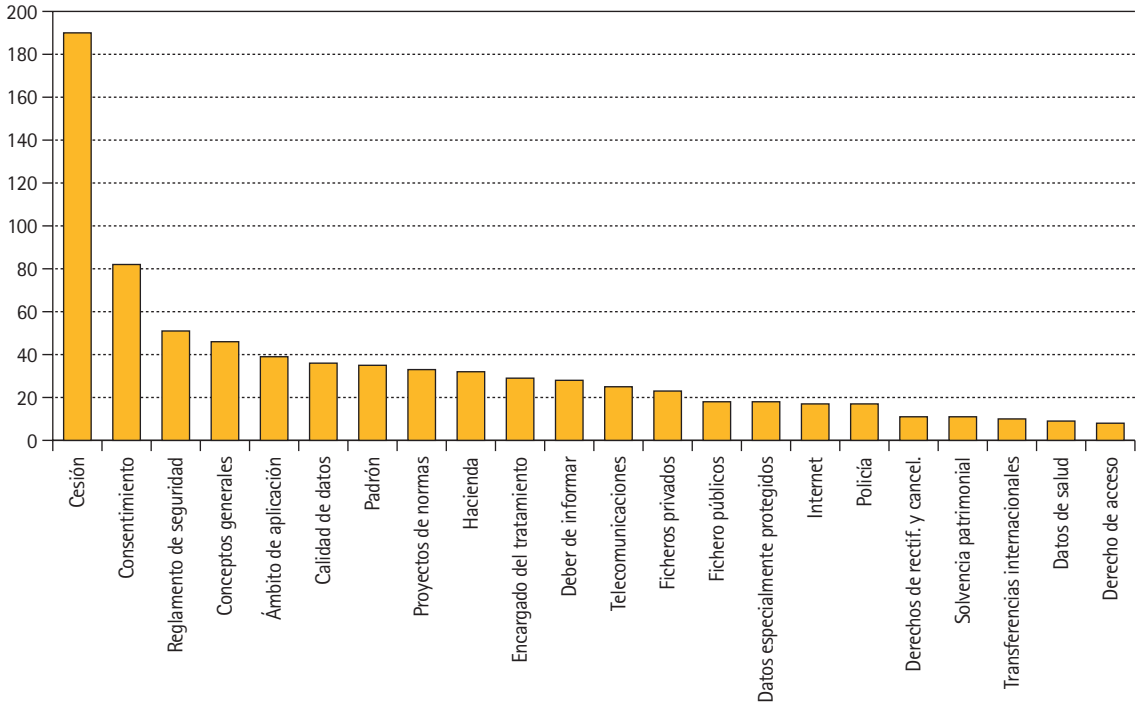


Finalmente, en lo referente a la distribución de consultas atendiendo a la materia sobre la que las mismas versan, puede observarse que predominan aquellas relativas a las cesiones de datos, en las que se mantiene la tendencia iniciada el año anterior, siendo muy elevadas las relativas a cesiones entre Administraciones Públicas, consecuencia de la modificación operada en la LOPD en este concreto aspecto por la Sentencia del Tribunal Constitucional 292/2000.

Se ha incrementado ligeramente 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, suscitándose una gran diversidad de cuestiones, generalmente de carácter interpretativo.

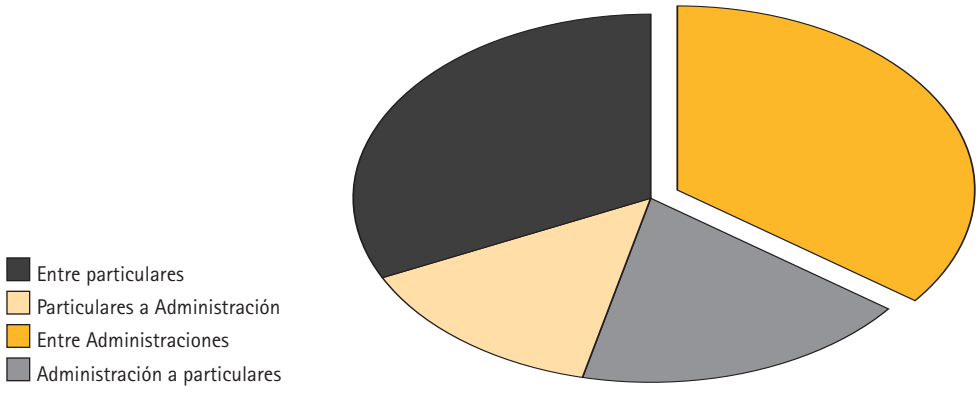
También, como se indicó anteriormente, resulta significativo el aumento de las cuestiones relacionadas con el sector de las comunicaciones electrónicas, así como el tratamiento de datos por parte de las Fuerzas y Cuerpos de Seguridad y por la Administración Tributaria. Por último, cabe destacar el incremento de 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.

CONSULTAS POR MATERIAS



Dado que, como se ha indicado, las consultas relativas a cesiones de datos siguen siendo las más abundantes, y siguiendo la sistemática ya planteada en Memorias anteriores, la distribución de los supuestos planteados atendiendo a la naturaleza pública o privada del cedente y del cesionario, es la siguiente:

CONSULTAS SOBRE CESIONES DE DATOS SEGÚN SU PROCEDENCIA Y DESTINO



2.2. Estudio de las cuestiones más relevantes planteadas por los responsables de ficheros o tratamientos

Como viene 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 más significativas.

2.2.1. Vigencia de la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995

Se planteó por una determinada empresa si es necesaria la autorización del Director de la Agencia para llevar a cabo una transferencia internacional de datos a un tercer Estado no miembro de la Unión Europea ni del Espacio Económico Europeo y respecto de cuyo nivel de protección de datos no existe Decisión alguna por parte de la Comisión Europea, dado que dicho Estado figura en la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995, por la que se declaran los Estados que ofrecen un nivel de protección de datos equiparable al establecido en la legislación española.

Sentado todo lo anterior, debe analizarse detenidamente si la competencia y criterios que sustentaban la adopción de la Orden de 2 de febrero de 1995 han de considerarse confirmados tras la entrada en vigor de la LOPD, lo que determinaría la aplicación de su Disposición transitoria tercera.

Tanto la derogada LORTAD como la vigente Ley Orgánica 15/1999 parten del concepto de que será admisible la transferencia internacional (sin requerir autorización específica del Director de la Agencia de Protección de Datos) en los supuestos en que el nivel de protección de datos en el país de destino sea «equiparable» al establecido en la Ley.

Si bien una mera lectura de estos preceptos permitiría considerar que, reproducido el precepto en una y otra norma, su contenido es el mismo, lo que induciría a considerar vigente la Orden citada, es necesario tener en cuenta que el término «equiparable» se predica de dos normas que, en ciertos aspectos, resultan ser distintas, toda vez que la Ley Orgánica 15/1999 viene a introducir en nuestro ordenamiento jurídico determinados principios en materia de protección de datos personales que hasta su entrada en vigor no aparecían recogidos en la legislación española.

En particular, es relevante tener en consideración cómo la nueva Ley Orgánica vino a reforzar los principios de consentimiento y finalidad, ejes esenciales de la protección de datos,

exigiendo requisitos más rigurosos para considerar cumplida la norma por parte de los responsables de los ficheros en estos casos. Así, desaparece la admisibilidad del consentimiento presunto, reforzándose los requisitos del consentimiento, que habrá de ser, en línea con lo exigido en la Directiva 95/46/CE, «libre, inequívoco, específico e informado».

Del mismo modo, se refuerzan las exigencias de información a los afectados, exigible en un mayor número de supuestos, así como, tal y como se indicó anteriormente, la necesidad de que cualquier finalidad del tratamiento resulte ser «determinada, explícita y legítima».

Además, la Ley regula con mayor detalle la figura del encargado del tratamiento, introduciendo requisitos más rigurosos que los contenidos en el artículo 27 de la LORTAD reconoce por primera vez el derecho de oposición, establece un régimen más pormenorizado del derecho de los afectados frente a las denominadas «decisiones personales automatizadas» y limita determinadas facultades hasta entonces ostentadas por los responsables de los ficheros de titularidad pública.

Por su parte, tras la doctrina sentada por el Tribunal Constitucional en sus sentencias 290/2000 y 292/2000, se establece un régimen aún más riguroso del derecho a la protección de datos, concebido ahora como derecho fundamental autónomo, y del principio de reserva de Ley en las limitaciones que puedan establecerse al ejercicio de este derecho.

Por todos estos motivos, si bien el artículo 33.1 de la LOPD reproduce el texto del artículo 32 de la LORTAD, ello no supone que dicho precepto haya de considerarse dotado de un mismo contenido normativo, dado que al establecer el mismo un término de referencia que, como se ha indicado, ha resultado alterado por las previsiones resultantes de la reforma de la Ley Orgánica, debe considerarse modificado el propio contenido del precepto, siendo así que resulta posible que la equiparabilidad que pudiera existir a partir del análisis comparativo de la legislación del país de destino en relación con la LORTAD no resulte tal tras la entrada en vigor de la LOPD.

Por ello, la mera inclusión de un determinado país en la Orden de 2 de febrero de 1995 no podría determinar automáticamente que su nivel de protección pueda ser considerado equiparable al previsto en la LOPD, aprobada casi cinco años después y reguladora de un régimen parcialmente distinto al de la norma derogada. Ello impide que pueda considerarse directamente aplicable la citada Orden en virtud de la Disposición transitoria tercera de la citada Ley Orgánica.

Por otra parte, debe indicarse que, en todo caso, el marco regulador de la protección de datos de carácter personal existente en el momento de adopción de la Orden de 1995 se encuentra modificado, además de en lo referente a determinados aspectos sustantivos de la protección de datos, como consecuencia de la adopción y entrada en vigor en octubre de 1998 de la Directiva 95/46/CE, que la propia Ley Orgánica 15/1999 viene a transponer

al ordenamiento español. Dicha Directiva impone determinadas conductas a las autoridades de control en lo que a la determinación del nivel adecuado o equiparable de protección se refiere.

Existe un último argumento de índole competencial que coadyuva a la consideración de la citada Orden de 2 de febrero de 1995 como derogada por la entrada en vigor de la Ley Orgánica 15/1999.

En efecto, la Orden fue dictada en virtud de la habilitación efectuada a favor del entonces Ministerio de Justicia e Interior por la Disposición final primera del Real Decreto 1332/1994. Dicha habilitación encontraba su justificación en la Disposición final primera de la Ley Orgánica 5/1992, que habilitaba al Gobierno para dictar las disposiciones necesarias para la aplicación y desarrollo de la misma.

Sin embargo, la Ley Orgánica 15/1999, aún conteniendo una habilitación similar en su Disposición final primera, introduce una fundamental modificación en lo que a la determinación del nivel adecuado de protección se refiere, al establecer el inciso primero del artículo 33.2 que «el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencias de datos».

En consecuencia, la mencionada Ley Orgánica atribuye a esta Agencia la competencia exclusiva para enjuiciar la existencia o inexistencia del mencionado nivel de adecuación, sin que dicho enjuiciamiento pueda efectuarse por la mera aplicación automática de una norma emanada de otro Órgano distinto, que delimite cuándo ha de entenderse procedente o improcedente dicha decisión.

En resumen, si bien en el momento de su adopción la Orden de 2 de febrero de 1995 fue dictada por Órgano competente para resolver sobre la existencia o inexistencia de adecuación, dicho Órgano perdió la competencia para decidir sobre esta cuestión con la entrada en vigor de la Ley Orgánica 15/1999, que atribuyó dicha competencia en exclusiva a la Agencia de Protección de Datos. Por este motivo, la Orden, válida en el momento de su adopción, devino contraria a lo establecido en la Ley Orgánica, lo que inequívocamente supone que la misma ha de entenderse derogada por ser contraria a la propia Ley, que atribuye en exclusiva a la Agencia la potestad de resolver sobre la existencia del nivel equiparable de protección en el Estado donde se encuentre el destinatario de los datos en una transferencia internacional.

En consecuencia, se ha indicado que la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995, y por extensión la Orden del Ministerio de Justicia de 31 de julio de 1998, por la que se ampliaba la relación contenida en la primera, deben entenderse derogadas por

la entrada en vigor de la Ley Orgánica 15/1999, sin que resulte de aplicación a este caso la previsión contenida en la Disposición transitoria tercera de la misma.

2.2.2. Competencias de la Agencia de Protección de Datos y las Autoridades de control creadas por las Comunidades Autónomas en materia de Registro

Se ha planteado por una Autoridad de control autonómica, de las previstas en el artículo 41.1 de la LOPD, el modo en que habría de resolverse el problema de que los ficheros sometidos a su ámbito de aplicación hayan de ser inscritos tanto en el Registro General de Protección de Datos como en el gestionado por la propia Agencia autonómica, considerando que el Registro ante el que debe efectuarse originariamente la inscripción es el de ésta última, siendo la inscripción en el Registro General de Protección de Datos «complementaria» de la anterior, a los meros efectos de publicidad.

Ello exige, lógicamente analizar la naturaleza de los registros existentes en ambas Autoridades de Control, así como su régimen jurídico y finalidad.

El deber de notificación y ulterior inscripción registral de los tratamientos de datos de carácter personal trae su causa de lo establecido en la Directiva 95/46/CE. En particular, el Considerando 48 de su Exposición de Motivos parte del principio de que «los procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva».

Esta vinculación entre la existencia misma de un registro de los tratamientos realizados en cada uno en los distintos Estados miembros y el deber de dar publicidad a dichos tratamientos, como garantía esencial de la posibilidad del ejercicio por los ciudadanos afectados de sus derechos derivados del derecho fundamental a la protección de datos de carácter personal, reconocido, entre otros instrumentos, por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, aparece claramente explicitada en el artículo 21 de la mencionada Directiva.

En el apartado 2 de dicho precepto, cuya rúbrica resulta ser precisamente «publicidad de los tratamientos», se impone a los Estados miembros la obligación de establecer «que la autoridad de control lleve un Registro de los tratamientos notificados con arreglo al artículo 18». Es necesario recordar que el artículo 21.1 establece claramente que «los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos» y que el artículo 21.2 delimita, en su párrafo segundo, la extensión que habrá de darse al registro público al que la misma se refiere, añadiendo expresamente el párrafo tercero que «el registro podrá ser consultado por cualquier persona».

Quiere todo ello decir que el Registro de los tratamientos, cuya existencia viene precisamente impuesta por la norma comunitaria rectora de la protección de datos de carácter personal, tiene por finalidad esencial el preservar la obligación de dar publicidad a dichos tratamientos. En consecuencia, tal finalidad no es meramente «complementaria» de otras atribuidas a los registros de tratamientos de datos de carácter personal, sino que constituye la verdadera justificación de su existencia.

Esta vinculación entre el Registro y el deber de publicidad de los tratamientos impuesto a los Estados miembros aparece también recogida en la Ley Orgánica 15/1999 que establece, en su artículo 14, el derecho de los afectados a conocer la existencia de los tratamientos, señalando que «cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita».

Posteriormente, los artículos 26 y 39 vienen a detallar el procedimiento de notificación de los ficheros o tratamientos al Registro General de Protección de Datos, así como el contenido del mismo.

En consecuencia, la Ley Orgánica 15/1999 atribuye al Registro General de Protección de Datos la esencial función, derivada de lo exigido por la Directiva 95/46/CE, de dar publicidad a los tratamientos de datos de carácter personal realizados en todo el territorio del Estado español, esto es, atribuye a ese Registro el cumplimiento de la finalidad que motiva su propia existencia a tenor de la Directiva Comunitaria.

Por este motivo, el artículo 23 del Estatuto de la Agencia de Protección de Datos establece inequívocamente que «el Registro General de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 13 a 15 de la Ley Orgánica 15/1992, de 29 de octubre». Debe tenerse en cuenta que dicha disposición ha de considerarse vigente, en virtud de lo dispuesto en la Disposición transitoria tercera de la Ley Orgánica 15/1999, si bien las referencias a la derogada Ley Orgánica 5/1992 deberán entenderse realizadas a aquélla.

A la luz de lo antedicho, el artículo 24 del Estatuto de esta Agencia impone la inscripción en el Registro de los ficheros que sean de titularidad de cualesquiera Administraciones Públicas, sin diferenciar entre los correspondientes a la Administración autonómica o local de aquellas Comunidades Autónomas que constituyeran, con arreglo a lo establecido en la derogada Ley Orgánica 5/1992 o en el artículo 41 de la vigente Ley Orgánica 15/1999 sus propias autoridades de control, regulando los artículos 5 y siguientes del Real Decreto

1332/1994, de 20 de junio, también vigente, los requisitos y procedimiento para proceder a la notificación y ulterior inscripción de los tratamientos en el Registro General de Protección de Datos.

Por otra parte, el artículo 41.1 de la Ley Orgánica 15/1999, delimita las competencias de las Autoridades de control de las Comunidades Autónomas, disponiendo que «las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido».

Además, esta norma se complementa con lo previsto en el artículo 41.2 que literalmente indica que «las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos».

Pues bien, de la delimitación del ámbito competencial de las autoridades de control que, en su día, fueran creadas por las distintas Comunidades Autónomas en virtud del título competencial contenido en el propio artículo 41, se desprende la existencia de dos límites importantes del mismo: uno en cuanto a las efectivas competencias que podrán ejercerse y otro en lo referente a los ficheros sobre los cuales cabrá ejercer la competencia.

A los efectos que aquí interesan, reviste especial importancia el primero de los límites señalados, dado que el propio artículo 41.1 impone expresamente que la habilitación competencial se extenderá, en relación con los ficheros incluidos en la norma, a todas las competencias de esta Agencia salvo las referentes a la elaboración de su Memoria Anual, elevada al Ministro de Justicia (artículo 37 k), la autorización y control de los movimientos internacionales de datos, tanto en cuanto a esta potestad en sí misma (artículo 37 l) como a lo que se refiera a la adopción de medidas de adecuación del tratamiento y ejercicio de la potestad sancionadora (artículos 37 f y 37 g) vinculadas con dicho movimiento internacional de datos y, lo que resulta esencial en este momento, a la competencia para «velar por la publicidad de la existencia de los ficheros de datos con carácter personal», así como la publicación periódica de «una relación de dichos ficheros con la información adicional que el Director de la Agencia determine» (artículo 37 j).

Quiere ello decir que el legislador ha querido atribuir en exclusiva a la Agencia de Protección de Datos la competencia derivada del cumplimiento de la previsión contenida en el artículo 21 de la Directiva 95/46/CE. Por este motivo sólo existirá un único Registro de

ficheros y tratamientos de datos de carácter personal constituido para cumplir la finalidad de publicidad exigida por la normativa comunitaria.

La razón de esta atribución, derivada directamente de lo dispuesto en el artículo 41.1 de la Ley Orgánica 15/1999, resulta lógica: si el principio de publicidad de los tratamientos va directamente vinculado al derecho de los ciudadanos a conocer la totalidad de los tratamientos de carácter personal, tal y como prescribe el artículo 14 de la Ley Orgánica 15/1999, este derecho quedará satisfecho con las mayores garantías para los ciudadanos en caso de que la publicidad proceda de una única fuente que, inmediatamente, incorpora cuantos tratamientos son objeto de notificación (en su caso, previa publicación de la disposición correspondiente), dado que dicha notificación es requisito necesario y previo a la existencia misma de las actividades de tratamiento de datos de carácter personal.

A esta conclusión coadyuva también la doctrina sentada por el Tribunal Constitucional, en su Sentencia 290/2000, de 30 de noviembre, que delimita el reparto competencial entre el Estado y las Comunidades Autónomas en esta materia. Según indica el Fundamento Jurídico 14 de la citada Sentencia, tras consagrar la naturaleza de derecho fundamental de la protección de datos de carácter personal:

> *«...la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas «ex» art. 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales.*
>
> *A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros».*

Cabría argumentar, en contra de la tesis hasta ahora sostenida y ratificada, como se ha podido comprobar, por la jurisprudencia Constitucional, que la consideración como exclusiva de la competencia de llevanza de un Registro que dé publicidad a los tratamientos de datos de carácter personal se contradice con la previsión contenida en el artículo 41.2 de la Ley Orgánica 15/1999, anteriormente transcrito.

No obstante, es necesario tener en consideración el tenor literal de este precepto, que aparece separado de aquél en que vienen expresamente a enumerarse las competencias que podrán ser ejercidas, en el ámbito objetivo que se delimita, por las Comunidades Autónomas. De dicho tenor literal se desprenden, cuando menos, dos consecuencias:

— La creación de registros de ficheros por parte de las Comunidades Autónomas es meramente potestativa.

— La finalidad de dichos registros no será la de dar publicidad a los tratamientos de datos de carácter personal, sino actuar como medio instrumental «para el ejercicio de las competencias que se les reconoce sobre los mismos».

Estas notas revisten una importancia fundamental en la resolución de la cuestión planteada. Ello se debe, en primer término, a que los registros no son considerados por el legislador como un instrumento necesario para el desempeño por las Comunidades Autónomas de las competencias que la Ley les atribuye, toda vez que podrán optar entre la creación de dichos registros o la utilización del propio Registro General de Protección de Datos, en virtud del principio de publicidad del mismo, consagrado por las normas españolas y comunitarias.

Por otra parte, en caso de que se opte por la creación de dichos registros, la naturaleza de los mismos diferirá completamente de la que justifica la existencia del Registro General de Protección de Datos: mientras este es el único registro creado directamente por el legislador para dar cumplimiento al deber de publicidad de los tratamientos consagrado por el artículo 21 de la Directiva 95/46/CE (que, insistimos, es la razón misma de la existencia de estos registros en los Estados miembros de la Unión Europea), los registros a los que se refiere el artículo 42.2 serán meros instrumentos internos que las Agencias Autonómicas podrán constituir para facilitar el desempeño de sus funciones. Serán en consecuencia, meros registros administrativos de los tratamientos, instrumentales de la actividad de la Agencia Autonómica, pero no se regirán por el principio de publicidad aplicable en exclusiva a la Agencia del Estado.

La legislación autonómica aplicable al caso consagra la obligación de inscripción de los tratamientos en el Registro de Ficheros de Datos de la Agencia Autonómica, añadiendo que es función de la misma velar por la publicidad de la existencia de los ficheros de datos de carácter personal.

No obstante, debe considerarse que lo establecido en la legislación autonómica deberá ser interpretado de forma conforme con la competencia exclusiva atribuida a la Agencia. Del mismo modo, las disposiciones contenidas en la legislación autonómica deberán armonizarse con el ámbito normativo contenido en la Ley Orgánica 15/1999.

Ello supone que, por una parte, la Comunidad ha optado por la creación del Registro al que se refiere el artículo 41.2 y que, por otra, la finalidad de dicho registro no podrá diferir de la establecida en aquel precepto, siendo por tanto la publicidad que la Agencia de Protección de Datos autonómica dé a los ficheros y tratamientos llevados a cabo por las Administraciones Públicas incluidas en el ámbito de aplicación de su normativa reguladora meramente complementaria o accesoria de la atribuida en exclusiva por el legislador a la Agencia de Protección de Datos a través del Registro General de Protección de Datos.

Por todo ello, no nos encontraríamos en este caso ante un supuesto de «doble inscripción registral» no prevista en nuestro Ordenamiento, sino ante un sistema en que existirá una inscripción obligatoria en el único registro al que la Ley otorga la función de dar publicidad a los tratamientos de datos de carácter personal, complementada con la inclusión de los tratamientos en el registro administrativo que la Comunidad Autónoma ha optado por crear, en cumplimiento de la facultad que le otorga el artículo 41.2 de la Ley Orgánica 15/1999, para finalidades meramente instrumentales para el mejor desempeño de las competencias del artículo 37 de la Ley Orgánica que la Agencia autonómica puede asumir (no para otras distintas).

Consecuencia de todo lo anterior es que no resulta posible considerar que la obligación de notificación y posterior inscripción en el Registro General de Protección de Datos de los tratamientos pueda quedar sometida a una previa notificación e inscripción en un Registro de ámbito autonómico, que enjuiciará, con carácter previo, la posibilidad de dicha inscripción.

Esta conclusión resulta especialmente relevante si se tiene en cuenta que algunos de los extremos que habrían de contenerse en la notificación del tratamiento deberán ser objeto de previa autorización de la Agencia de Protección de Datos, tal y como sucede en lo referente a la autorización de transferencias internacionales de datos de carácter personal.

Tampoco puede resultar de recibo la solución ofrecida, que implica la mera inscripción en el Registro General de Protección de Datos como consecuencia de la notificación periódica de los tratamientos inscritos en el Registro de Ficheros de la agencia autonómica, dado que, entre otras cosas, la inscripción del tratamiento en el Registro General es requisito previo indispensable para que pueda, efectivamente, llevarse a cabo el tratamiento de los datos de carácter personal.

A la vista de todo ello, el responsable del fichero estará obligado, en todo caso, a notificar la existencia del mismo a la Agencia de Protección de Datos, sin perjuicio de la obligación de aquél de notificar dicho tratamiento para su inclusión en el Registro de Ficheros de la autoridad autonómica, sin que ello suponga una «doble inscripción registral» en dos registros de la misma naturaleza, dado que la naturaleza de ambos registros es completamente dispar, procediendo la obligación de notificar el tratamiento a esta Agencia de normas aplicables en todo caso, por la expresa salvedad contenida en el artículo 41.1 de la Ley Orgánica 15/1999 a su artículo 37 j).

2.2.3. Cesión de datos de abonados a prestadores de servicios de emergencia. Diferencias con la cesión para elaboración de directorios

Se planteó a la Agencia si resulta conforme a las normas de protección de datos la comunicación a un Centro de Emergencias de los datos referidos a la totalidad de los abonados al servicio telefónico disponible al público, dado que la citada Entidad ha sido habilitada para la gestión del teléfono de emergencias 112. En particular, la consulta hacía referencia a la previsión contenida en la Directiva 96/19/CE que reconoce el derecho de los abonados a no figurar en los directorios telefónicos.

El problema se plantea en relación con los datos de aquellas personas que hubieran ejercido su derecho de no figurar en los directorios telefónicos, en los términos previstos en el artículo 67.2 del Real Decreto 1736/1998, reproducidos asimismo por el apartado 4 de la Norma tercera de la Orden del Ministerio de Ciencia y Tecnología de 26 de marzo de 2002, que establece las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

Sin embargo, a juicio de la Agencia, no se produciría una contradicción entre ambas normas por el hecho de que se faciliten al prestador del servicio telefónico de emergencia 112 los datos referentes a las personas que hayan ejercitado su derecho a no aparecer en las guías telefónicas o en los servicios de consulta telefónica, dado que el tratamiento llevado a cabo por los prestadores del servicio de información o de elaboración de guías y el desarrollado por las entidades a las que se encomienda la gestión del número de emergencias 112 resulta distinto.

Ello se basa en que la finalidad del tratamiento en uno y otro caso (prestación de servicios de directorio telefónico o información y atención del servicio de emergencias 112) difieren claramente: el primero persigue una finalidad meramente divulgativa, mientras que el segundo se deriva de la atribución otorgada a los distintos entes por la Administración competente para resolver situaciones de emergencia en las que la vida o la integridad del interesado o de terceros puede encontrarse en una situación de riesgo.

Por este motivo, dadas las distintas finalidades perseguidas con el tratamiento, el legislador comunitario y nacional resuelve de manera distinta el supuesto de colisión entre la privacidad de los afectados y la protección de la finalidad perseguida por el tratamiento.

En efecto, las normas nacionales y comunitarias reguladoras del servicio de telecomunicaciones incluyen previsiones sobre la prestación del servicio de directorio e información telefónica en que se reconoce, como norma fundamental, el derecho del afectado a no aparecer en tales directorios o servicios de información. Ello se funda en que, ante la coli-

sión que podría producirse entre la prestación del servicio y el derecho de los terceros a conocer los datos del afectado y el derecho de este último a su intimidad, el legislador comunitario, y posteriormente el nacional, han considerado la prevalencia de este último, como más digno de protección que el potencial derecho a conocer los datos publicados en el directorio.

Sin embargo, estas mismas normas, al regular la existencia del servicio de emergencias 112, han venido a considerar prevalente el derecho de salvaguardar la integridad de personas o bienes del afectado o de terceras personas e incluso el derecho a atender una necesidad vital del afectado o terceros (que, como ya indicamos, habilita el tratamiento de datos de carácter personal sin el consentimiento del afectado, tanto en la Directiva como en la Ley Orgánica 15/1999), sobre el mencionado derecho a preservar esa intimidad.

Esta diferenciación encuentra su reflejo en la consagración por el artículo 54.3 de la Ley General de Telecomunicaciones del derecho del abonado a no figurar en los directorios telefónicos. Pero este derecho no pude identificarse en modo alguno con un derecho del abonado a que no se comuniquen a los entes competentes sus datos con el fin de poder atender a situaciones de emergencia.

Así, en desarrollo de la meritada Ley, y del Real Decreto 1736/1998, la Orden del Ministerio de Ciencia y Tecnología de 26 de marzo de 2002 establece dos supuestos claramente diferenciados en cuanto a la cesión o comunicación de los datos de los abonados al servicio telefónico, en atención al destinatario de los datos:

- En cuanto a la cesión para las entidades habilitadas para prestar el servicio de consulta telefónica, la Comisión del Mercado de las Telecomunicaciones, facilitará a las mismas «la información actualizada que puedan utilizar en sus bases de datos, a la que se refiere el apartado tercero» (número 1 del apartado decimoquinto), en el que se incluye el derecho del interesado a «que se le excluya de las guías telefónicas o de los servicios de consulta telefónica sobre números de abonado» (número 4). De este modo, los datos de quienes desean ser excluidos de este servicio podrían no ser facilitados a estas entidades.

- Sin embargo, en lo referente a la comunicación de los datos a las entidades que presten servicios de llamadas de urgencia a través del número 112 y a las entidades que determine la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información por prestar servicios de llamadas de urgencia a través de números cortos, el número 2 del propio apartado decimoquinto de la Orden dispone que la Comisión del Mercado de las Telecomunicaciones comunicará, previa petición, «la información actualizada a la que se refiere el punto 1 del apartado decimocuarto», según el cual los operadores facilitarán a la Comisión los datos de «todos sus abonados», sin distinguir entre quienes desean o no figurar en los directorios telefónicos.

En consecuencia, la norma establece una clara distinción entre ambos supuestos, basada en el hecho de que el derecho del abonado a no figurar en el directorio no implica la posibilidad de que el mismo pueda ejercer un derecho a que sus datos no se faciliten a las entidades prestadoras del servicio telefónico de urgencia.

Por todo ello, la comunicación podrá extenderse, tal y como se indica en la Orden de 26 de marzo de 2002 a los datos de «todos los abonados».

No obstante, es preciso indicar que la limitación al ejercicio del derecho del abonado impuesta por la norma no es absoluta, sino que, en línea con lo que se ha venido razonando, se hace depender explícitamente de la utilización de los datos para la finalidad de prestación del servicio de urgencia. Por este motivo, el apartado decimoquinto de la Orden dispone en su punto 2 que «los datos obtenidos serán utilizados exclusivamente como soporte para la efectiva prestación de los servicios de atención de llamadas de urgencia, siendo responsabilidad de la entidad prestataria el adecuado uso de los mismos, que estará sometido a la legislación vigente sobre protección de datos de carácter personal».

2.2.4. Utilización del dato de afiliación sindical en los procedimientos de despido

Se ha planteado si resulta conforme con lo establecido en la LOPD la utilización por parte del empresario del dato referente a la afiliación sindical del trabajador, facilitado por éste a fin de que por la empresa se proceda al pago de la cuota sindical, con la finalidad de que el empresario pueda comunicar a los representantes del sindicato a que el trabajador se halle afiliado la iniciación de un procedimiento de despido disciplinario contra aquél.

Como regla general, el dato de la afiliación sindical tiene la naturaleza de dato especialmente protegido, en los términos previstos en la Ley Orgánica 15/1999, disponiendo el artículo 7.2 de la misma, en su inciso primero, que «sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias».

Por otra parte, el artículo 4.2 de la Ley, «los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos».

Esta previsión, debe interpretarse de forma armonizada con lo establecido en el artículo 7.2 precitado y con lo que dispone, en general, el artículo 6.1 de la Ley Orgánica, cuando esta-

blece que «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa».

Dado que la Ley no identifica qué ha de entenderse por «fin compatible», debe analizarse la existencia de dicha compatibilidad en cada supuesto de hecho que se plantee, determinando si a la luz de las disposiciones aplicables a cada caso y de las circunstancias del mismo cabe considerar que esa finalidad que se alega como compatible resulta lícita a la luz de las normas aplicables y si la misma guarda una adecuada relación con la finalidad que justificó el tratamiento de los datos.

En el supuesto objeto de análisis, el artículo 10.3.3 de la Ley Orgánica 11/1985, de 2 agosto, de Libertad Sindical dispone que «Los delegados sindicales, en el supuesto de que no formen parte del comité de empresa, tendrán las mismas garantías que las establecidas legalmente para los miembros de los comités de empresa o de los órganos de representación que se establezcan en las Administraciones públicas, así como los siguientes derechos a salvo de lo que se pudiera establecer por convenio colectivo: Ser oídos por la empresa previamente a la adopción de medidas de carácter colectivo que afecten a los trabajadores en general y a los afiliados a su sindicato en particular, y especialmente en los despidos y sanciones de estos últimos».

En ejecución de este derecho, el artículo 115.2 de la Ley de Procedimiento Laboral, aprobada por Real Decreto Legislativo 2/1995, de 7 abril, dispone que «A los efectos de lo previsto en el número anterior serán nulas las sanciones impuestas a los representantes legales de los trabajadores o a los Delegados sindicales por faltas graves o muy graves, sin la previa audiencia de los restantes integrantes de la representación a que el trabajador perteneciera así como a los trabajadores afiliados a un Sindicato, sin dar audiencia a los Delegados sindicales», debiendo constar esta circunstancia en la demanda de despido, según dispone el artículo 114.

Por último, el artículo 55.1, párrafo cuarto, del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 1/1995, de 24 marzo, impone una carga al empleador, al señalar que «si el trabajador estuviera afiliado a un sindicato y al empresario le constare, deberá dar audiencia previa a los delegados sindicales de la sección sindical correspondiente a dicho sindicato».

Como puede comprobarse, el legislador ha considerado como único requisito necesario para que proceda la comunicación a los representantes sindicales del trabajador inmerso en un expediente de despido de esta circunstancia que al empresario «le constare» dicha afiliación sindical, sin especificar el motivo del que pueda proceder dicha constancia. En este sentido, la Sentencia del Tribunal Constitucional 30/1992 señala en su Fundamento Jurídico 6 que «dicha obligación (de notificación a los representantes sindicales) sólo puede sur-

gir cuando el trabajador, al menos, ha puesto en conocimiento del empresario su condición de afiliado a un sindicato».

También por este motivo, la Sentencia del Tribunal Superior de Justicia de Andalucía, con sede en Málaga, de 5 de febrero de 1991 declaró que era «indudable que al organismo demandado necesariamente le constaba la condición de afiliado del actor a dicha central sindical desde el momento en que en la nómina le efectuaba el descuento de la cuota sindical correspondiente» y la Sentencia del Tribunal Superior de Justicia de Galicia, de 31 de mayo de 1996 declara no haber lugar a la nulidad del despido por cuanto no se solicitó dicha deducción.

A la vista de todo lo anterior, no cabe duda que de las normas vigentes y de la interpretación que de las mismas realizan los distintos Órganos Jurisdiccionales y el propio Tribunal Constitucional se desprende que el mero conocimiento del hecho de la afiliación por haberse solicitado la deducción de la cuota sindical es suficiente para que el empresario esté obligado a la notificación del expediente de despido a la representación del sindicato al que pertenezca el trabajador impuesta por el Estatuto de los Trabajadores, so pena de la declaración de nulidad del despido.

Por ello, se considera que la utilización del dato de la afiliación para comunicar a la representación sindical del sindicato al que pertenece el trabajador la notificación del despido del mismo supondrá la utilización del dato para un fin compatible con el que motiva el tratamiento, siendo dicha utilización conforme a lo dispuesto en la Ley Orgánica 15/1999.

2.2.5. Naturaleza del dato de opción por la asignatura de religión

Se ha formulado una consulta cuestionando si el dato relativo al hecho de que un determinado alumno de un centro docente opte por cursar la asignatura de religión o la alternativa prevista por la Ley ha de ser considerado como dato especialmente protegido a los efectos previstos en la LOPD.

Como punto de partida, el artículo 7.2 de la Ley Orgánica 15/1999 dispone que «sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias», prohibiendo el artículo 7.4 «los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual». Estas previsiones deben ponerse en conexión con lo establecido en el artículo 7.1 de la Ley Orgánica, a cuyo tenor «nadie podrá ser obligado a declarar sobre su ideología, religión o creen-

cias». Dicho precepto es una mera reproducción de lo establecido, a su vez, en el artículo 16.2 de la Constitución.

De este modo, ha de considerarse que los datos a los que se refiere el artículo 7.2 de la Ley Orgánica 15/1999 son aquéllos que efectivamente se encuentran directamente vinculados con las creencias religiosas, filosóficas, políticas o morales de la persona, protegidas constitucionalmente a través del derecho fundamental a la libertad ideológica, religiosa y de culto, consagrado por el artículo 16.1 de la Constitución.

Sentados así los términos de interpretación de lo establecido en el artículo 7.2 de la Ley Orgánica 15/1999, debe ahora plantearse si el hecho de cursar la asignatura de religión, o el hecho de no cursarla, suponen la revelación de un dato protegido por el citado derecho fundamental, que coadyuva a la especial protección que también confiere la LOPD, es decir, si ese dato revela efectivamente las convicciones religiosas de la persona a la que se refiere.

Pues bien, el hecho mismo de cursar la asignatura de religión no revela necesariamente que el estudiante profese las creencias a las que tal asignatura se refiere, del mismo modo que el hecho de no cursarla no revela la inexistencia de esas creencias, sino que tal circunstancia puede deberse al estudio de la religión en otros foros distintos del escolar. Es decir, a nuestro juicio, lo único que revela el dato de optar por cursar la asignatura de religión sería el interés del alumno por conocer los principios, historia y preceptos de la misma, sin que ello implique una efectiva confesionalidad del mismo, a cuya declaración no podría encontrarse obligado.

Por este motivo, el dato relacionado con el hecho de que el alumno curse la asignatura de religión, no vinculada a la participación del alumno en un rito relacionado con una religión determinada (lo que sí implicaría que el individuo profesa dicha creencia religiosa), no puede ser considerado por sí mismo un dato que revele inmediatamente las creencias religiosas del afectado, por lo que su régimen no se encuentra sometido a lo establecido en las normas que se citaron anteriormente, dado que el dato no tendría la naturaleza de especialmente protegido.

2.2.6. Cesión del dato del NIF del afectado por los bancos en que aquél domicilia sus pagos

Se formuló por un operador de telecomunicaciones una consulta a fin de obtener el parecer de la APD sobre si resulta conforme a lo establecido en la LOPD que por aquél se solicitase de las entidades bancarias en que sus clientes hubieran domiciliado el pago de su factura telefónica el dato referente a su Número de Identificación Fiscal en aquellos supuestos en que la consultante careciera del mismo o dicho dato fuera erróneo.

La solicitud del dato del NIF de los abonados se funda en lo dispuesto en el artículo 13.1 del Real Decreto 338/1990, de 9 de marzo, que regula la composición y forma de utilización del número de identificación fiscal, según el cual «los sujetos pasivos u obligados tributarios deberán consignar el Número de Identificación Fiscal de otras personas o Entidades, con quienes establezcan relaciones económicas o profesionales, en declaraciones, comunicaciones o documentos con trascendencia fiscal, de acuerdo con lo dispuesto en este Real Decreto o en otras disposiciones de naturaleza tributaria».

De este modo, la consultante no podría cumplir su obligación de consignar el número de identificación fiscal de sus clientes, ante la negativa, expresa o tácita, de los mismos a facilitarlo.

El mencionado Real Decreto es desarrollo de lo dispuesto en el artículo 113 de la Ley 33/1987, de 23 de diciembre, de Presupuestos Generales del Estado para 1988, por el que se crea y regula el Número de Identificación Fiscal. El párrafo tercero del apartado 1 del citado precepto dispone que «reglamentariamente se regulará la composición del número de identificación fiscal y la forma en que deberá utilizarse en aquellas relaciones de naturaleza o con trascendencia tributaria».

En consecuencia, la mencionada Ley habilita expresamente un desarrollo reglamentario que delimite los supuestos en que, en el ámbito de los negocios celebrados por su titular, deberá facilitarse o comunicarse a quien mantenga con el una relación con trascendencia tributaria, el dato correspondiente al número de identificación fiscal.

El artículo 13 del Real Decreto 339/1990 dispone, en cumplimiento de la habilitación efectuada por el artículo 113.1 de la Ley 33/1987, y en relación con su propio artículo 13.1, que «Para cumplir lo dispuesto en el apartado anterior, los sujetos pasivos u obligados tributarios exigirán de las personas o Entidades con quienes se relacionen que les comuniquen y acrediten su Número de Identificación Fiscal, debiendo éstas facilitarlo».

En resumen, el citado precepto impone a cualquier persona o entidad que se relacione con un sujeto pasivo u obligado tributario la obligación de comunicar al mismo su número de identificación fiscal, dentro de los términos habilitados por el artículo 113.1 de la Ley 33/1987. Es decir, el número de identificación fiscal deberá ser comunicado en cualquier acto que pudiera revestir trascendencia tributaria, entre los que se encontrará, en todo caso, el abono de un determinado servicio, como el telefónico, dado que el mismo se encuentra sometido al impuesto sobre el valor añadido, según las normas de este impuesto, lo que implica su trascendencia a efectos tributarios.

Consecuencia de lo anterior es la concurrencia de una obligación de facilitar el dato del número de identificación fiscal en aquellos abonados que se han negado previamente a su facilitación.

Dicho lo anterior, y teniendo en cuenta la falta de comunicación del número de identificación fiscal por los propios afectados, se plantea si las entidades encargadas, en nombre y por cuenta del propio abonado, de efectuar el abono del servicio telefónico podrían transmitir a la consultante el dato referente a dicho número de identificación fiscal.

Las entidades operan en virtud de un mandato de pago efectuado por el propio abonado que solicita de la entidad bancaria su realización. En consecuencia, se produce en este caso un mandato a la entidad para dar cumplimiento a la prestación exigida por el contrato celebrado por aquella entidad a la que se efectúa el pago, es decir, para consumar la relación que vincula al cliente de la entidad crediticia con la persona o entidad con la que se encuentra obligado en virtud de una relación contractual o meramente negocial.

Pues bien, dado que la entidad bancaria viene a dar cumplimiento a la prestación derivada de tal relación jurídica, dicho cumplimiento habría de cumplir los requisitos que las Leyes establezcan para que pueda efectivamente considerarse cumplida en plenitud la obligación del cliente.

De entre dichos requisitos, como se ha indicado anteriormente, el artículo 13.2 del Real Decreto 339/1990 impone a quienes establezcan con cualquier sujeto pasivo u obligado tributario una relación con trascendencia tributaria la obligación de facilitar su número de identificación fiscal. De este modo, para que la entidad bancaria dé adecuado cumplimiento al mandato de pago otorgado, será preciso que, dada su trascendencia tributaria, facilite al destinatario del pago el número de identificación fiscal del cliente, relacionado con dicha entidad, en aquellos supuestos en que la misma no tuviera conocimiento de ese dato, tal y como sucede en este caso, dado que es la Ley (que prevé la habilitación reglamentaria de los supuestos en que deba ser facilitado el NIF) la que daría cobertura a la cesión, encontrándose ésta amparada en el artículo 11.2 a) de la LOPD.

En todo caso, sería necesario que el tratamiento que realice la consultante del dato resultante de la cesión se ajuste estrictamente a la finalidad que motiva la misma, es decir, el cumplimiento de lo previsto en las normas reguladoras del número de identificación fiscal, de forma que este dato sea únicamente empleado a los fines previstos en dichas normas.

2.2.7. Procedimiento para la exención del deber de informar (artículo 5.4 LOPD)

Se recibió en la Agencia de Protección de Datos un escrito en que se solicitaba que por el Director de la Agencia de Protección de Datos se resuelva sobre la procedencia de aplicar a la entidad solicitante la excepción al deber de información a los afectados, contemplada en el artículo 5.4 de la LOPD, al suponer dicha notificación «un esfuerzo desproporcionado en consideración al número de interesados».

El artículo 5.5 de la Ley dispone que «no será de aplicación lo dispuesto en el apartado anterior (referido al deber de información a os afectados cuando los datos no sean recabados de los mismos) (...) cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias».

De ello se desprende que la apreciación de la excepción indicada sólo será posible a través de un acto administrativo de la Agencia en que se decida acerca de la procedencia o improcedencia de la excepción alegada en cada caso concreto. Dicho acto implicará la tramitación del correspondiente procedimiento administrativo, con todas las garantías establecidas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y que habrá de someterse a las reglas previstas en su Título VI, dada la aplicación supletoria de la misma prevista por el artículo 35.2 de la Ley Orgánica 15/1999.

Se tratará en todo caso de un procedimiento iniciado por la propia solicitud del interesado, de modo que no será necesaria la adopción de un acuerdo de iniciación de oficio.

En la tramitación del procedimiento deberá requerirse al solicitante para que acredite efectivamente la desproporcionalidad del esfuerzo que conllevaría la práctica de la notificación. En particular, la Ley Orgánica 15/1999 establece como criterios que habrán de ser ponderados por la Agencia para valorar si procede o no aplicar la excepción del artículo 5.4 la antigüedad de los datos, el número de afectados y las medidas compensatorias que se adopten por el responsable del tratamiento.

Por ello, sería necesario que en la fase probatoria se cuantificara realmente el coste que conllevaría la notificación a los afectados y que, durante esta misma fase, se solicitara la expresión del modo en que se adoptarán, en su caso, las medidas compensatorias.

Por otra parte, es necesario resaltar que de lo dispuesto en el artículo 5.4 se desprende que la facultad de decisión de esta Agencia se limitará a determinar si, dadas las circunstancias del caso (y, en particular, las previstas en la propia norma) la notificación implicaría un esfuerzo desproporcionado.

En consecuencia, del tenor de la norma no se desprende que sea la Agencia de Protección de Datos la que haya de resolver sobre las medidas compensatorias que hayan de adoptarse, sino únicamente sobre la suficiencia de las medidas que se hayan propuesto. Por esta razón, no parece que la Resolución pueda aprobar o no la medida propuesta, sino simplemente declarar si es posible aplicar la excepción a la vista de tal medida.

Por este motivo en caso de que se considere que la medida no fuera suficiente, esta circunstancia debería quedar claramente expresada en la propuesta de Resolución, en la que además podría señalarse (a fin de garantizar la debida celeridad de procedimiento, impuesta por el artículo 75 de la Ley 30/1992) cuál sería el criterio de la Agencia para delimitar las medidas compensatorias que, en su caso, pudieran ser suficientes para estimar la solicitud planteada, a fin de que el interesado pudiera, en el trámite de audiencia concedido por el artículo 84 de la Ley 30/1992 aclarar, si lo estima necesario, las medidas compensatorias propuestas o si procede proponer nuevas medidas.

Finalmente, la Resolución del procedimiento debería ser dictada por el Director de la Agencia de Protección de Datos, dado que, pese a que el artículo 12 del Estatuto de la Agencia de Protección de Datos no incluye referencia alguna a este procedimiento, si cabría apreciar su competencia en virtud de la función de Dirección y Representación de la Agencia atribuida por el artículo 36.1 de la Ley Orgánica 15/1999, siendo dicha Resolución susceptible de recurso contencioso-administrativo ante la Audiencia Nacional, de conformidad con lo establecido en el apartado 5 la Disposición Adicional cuarta de la Ley 29/1998, de 13 de Julio, reguladora de la Jurisdicción Contencioso Administrativa.

2.2.8. Cesión de datos para la realización de un estudio sociológico

Se ha planteado una consulta sobre la posibilidad de que sean comunicadas por parte de varias Universidades públicas a una persona o entidad que tenga prevista la realización de un proyecto de Investigación sociológico determinados datos personales, con la finalidad de delimitar a las personas concretas que serán contactadas para la efectiva realización del estudio. La consultante amparaba la cesión en el artículo 11.2 e) de la LOPD, según el cual sería posible la cesión de los datos sin contar con el consentimiento de los afectados cuando la misma se produjera entre Administraciones Públicas y se realizara con fines históricos, científicos o estadísticos.

Para que fuera posible la aplicación del supuesto invocado es preciso, en primer lugar, que exista una adecuación subjetiva del supuesto de hecho al que se pretenda aplicar. Ello implicaría que tanto el cedente como el cesionario tuviesen encaje en el concepto jurídico de Administración Pública.

En este caso, dicho presupuesto no planteaba problemas en el caso del cedente, pues se trataría en todo caso de universidades públicas, pero sí plantea ciertas dudas en el supuesto del cesionario. En caso de que el destinatario fuese un Instituto Universitario de Investigación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, indica que los mismos se configuran como centros dedicados a la investigación científica y técnica o a la creación artística, que se rigen por dicha Ley y por sus propios estatutos o convenios de

creación o adscripción, y cuya creación ha de ser acordada por la Comunidad Autónoma, bien a propuesta del Consejo Social o bien por propia iniciativa con el acuerdo del referido Consejo, en todo caso previo informe del Consejo de Gobierno de la Universidad (artículo 10. 3 en relación con el 8. 2).

Pues bien, cabe indicar que únicamente en el supuesto de que el proyecto científico se desarrollase por un Instituto Universitario a título institucional podrían ser de aplicación los artículos 21. 1 y 11.2 e) de la LOPD, siendo en caso contrario (desarrollo del mismo a título personal por personal docente universitario, adscrito o no al mismo) de aplicación el artículo 11.1 LOPD, que exigiría el consentimiento del afectado para la cesión de los datos.

Establecido lo anterior, es necesario analizar si la cesión analizada puede tener encaje en el citado supuesto, esto es, cesión entre Administraciones públicas para el tratamiento de los datos con un fin científico.

El término «científico» desde un punto de vista semántico implica pertenencia a una ciencia. Tal expresión, entendida literalmente, tiene una amplitud omnicomprensiva que implicaría la posibilidad de conectar prácticamente cualquier tratamiento de datos personales con una especialidad científica, tanto referida a las ciencias sociales como a las naturales. Así, incluso un estudio de mercado, de publicidad, o de técnicas comerciales o publicidad tendría o podría establecérsele una conexión con una especialidad o rama del conocimiento (ciencias económicas, ciencias de la información, etc.).

Parece en consecuencia lógico que la interpretación auténtica de tal precepto deba efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la LOPD. Así el artículo 4 de la misma establece en su apartado primero que «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».

De este modo, los artículos 21. 1 y 11. 2 e) de la LOPD deben ser interpretados a la luz de este principio y de la doctrina consagrada por la Sentencia del Tribunal Constitucional 292/2000, que configura la protección de datos como un auténtico derecho fundamental. Cuando dichos preceptos aluden al fin científico del tratamiento de los datos personales como supuesto que al excluir el consentimiento previo a la cesión de los mismos, están limitando y excluyendo tal poder decisorio y dispositivo de los ciudadanos que les es inherente según se ha visto. No todo proyecto intitulado «científico» amparará la cesión de datos prevista en los preceptos indicados, debiéndose analizar detenidamente y de forma individualizada a fin de determinar si efectivamente, a la vista del ente que desarrolla la investigación, el fin de la misma y la proporcionalidad de la intromisión o limitación del

derecho considerado que dicho estudio conlleve, puede efectivamente considerarse procedente la aplicación de tales preceptos de la Ley Orgánica 15/1999. Se trataría en consecuencia de considerar las circunstancias concretas que concurrirían en cada supuesto sometido a la opinión de la Agencia de Protección de Datos, teniendo en cuenta, en especial, la normativa específica que pudiese resultar de aplicación al mismo (como por ejemplo sucedería en el caso de actividades científico-sanitarias).

En el caso sometido a informe se apreció, en primer lugar, que los datos que se tratan de obtener deben considerarse adecuados y proporcionados a la finalidad del estudio que se pretende desarrollar. Además, la materia objeto de análisis ha sido considerada relevante por la Comisión Interministerial de Ciencia y Tecnología que decidió incluir el proyecto en el Plan I+D+I.

Por otra parte, la obtención de dichos datos simplemente tenía por objeto determinar el ámbito subjetivo del estudio en personas concretas, con las que posteriormente los investigadores se pondrían en contacto para solicitarles datos adicionales o analizar su situación personal, lo cual en todo caso va a requerir el consentimiento y la colaboración de los mismos. Del mismo modo, si dicho consentimiento no se obtuviese finalmente, los datos personales de los interesados que los hubiesen denegado deberían en todo caso ser cancelados de manera inmediata, ya que habría desaparecido la finalidad que dio fundamento legal a su tratamiento.

Por todo ello, atendiendo a las circunstancias concurrentes en ese caso concreto, se consideró que la comunicación planteada tendría cabida en el régimen impuesto por la LOPD sin necesidad de recabar con carácter previo el consentimiento de los afectados.

2.2.9. Publicación en Internet de datos históricos

Se planteó a la Agencia si resulta conforme a la LOPD la difusión en Internet de una base de datos de nombramientos de jefes, oficiales, suboficiales y miembros de los Cuerpos de Seguridad en los años de la Guerra Civil española, partiendo del hecho de que dicha publicación sólo incorporará los datos de nombre y apellidos, año del nombramiento y publicación oficial en que apareció el mismo.

Tras indicarse que la publicación de los datos supondría una cesión de los mismos, se recordó que el artículo 11.1 de la LOPD 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 legítimas del cedente y del cesionario con el previo consentimiento del interesado» y que el consentimiento sólo podrá verse exceptuado en los supuestos establecidos en el art. 11.2, de los que resultan relevantes a efectos de este caso los apartados a) y e) referido el primero a la existencia de una norma habilitante que

tenga rango de Ley, y el segundo a la cesión entre Administraciones Públicas fundadas en motivos históricos, científicos o estadísticos.

Dado que la difusión se va a efectuar a través de Internet, siendo destinatarios de la misma tanto las Administraciones Públicas como los ciudadanos, no será posible invocar la excepción contenida en el citado art. 11.2 e), planteándose si la misma podrá fundarse en lo establecido en el art. 11 .2 a), siempre y cuando la cesión se refiera a documentos que, según lo estipulado en las Leyes, pudieran dar lugar a la existencia de un interés histórico en su conocimiento.

En este sentido, el art. 57. 1c) de la Ley 16/1985 de 25 de Junio reguladora del Patrimonio Histórico Español establece que «los documentos que contengan datos personales de carácter policial, procesal, clínico, o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos».

A la vista de este precepto, y siempre que se cumplan los requisitos de plazo que el mismo establece, sería posible la consulta pública del documento, siendo así admisible su divulgación a través de Internet.

En los demás supuestos, es decir cuando los documentos no tengan la antigüedad exigida por la Ley del Patrimonio Histórico Español para que los mismos puedan ser considerados como de interés histórico, será necesario recabar el consentimiento de los afectados para la publicación del documento, dado que en este caso, dicha divulgación no se encontraría amparada en ninguna disposición con rango de Ley, al limitar el art. 37.2 de la Ley 30/1992 el acceso a dichos documentos al propio interesado.

2.2.10. Requisitos para la inclusión de datos de abonados en directorios de telefonía móvil

Se ha planteado por un operador de telefonía móvil si conforme a la LOPD y la normativa vigente en materia de telecomunicaciones, es posible incluir directamente los datos de sus abonados en guías telefónicas, con excepción de aquellos que hayan solicitado expresamente su exclusión, o para ello es preciso obtener previamente el consentimiento previo de cada uno de sus clientes.

En este sentido debe previamente recordarse como la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en relación con la inclusión de abonados en las guías telefónicas,

establece en primer lugar, entre las prestaciones que deben integrar el servicio universal de telecomunicaciones la recogida en el artículo 37. 1 b), consistente en que «que los abonados al servicio telefónico dispongan, gratuitamente, de una guía telefónica, actualizada e impresa y unificada para cada ámbito territorial. 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».

A su vez, el artículo 50 recoge el principio de protección de datos personales (con una remisión a la LORTAD que hoy debe entenderse efectuada a la Ley Orgánica 15/1999) en la que, en dicha materia, remite a las disposiciones reglamentarias de carácter técnico que puedan dictarse posteriormente, al afirmar que «los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal, conforme a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, en las normas dictadas en su desarrollo y en las normas reglamentarias de carácter técnico, cuya aprobación exija la normativa comunitaria en materia de protección de los datos personales».

Debe estarse pues, además de a la normativa específica de protección de datos, a lo dispuesto en las normas reglamentarias de desarrollo de dicha Ley 11/1998 en relación con la inclusión de datos personales en guías de abonados.

Así, y en primer lugar, la Orden del Ministro de Ciencia y Tecnología, de 21 de diciembre de 2001 (BOE 28 de diciembre), por la que se regulan determinados aspectos del Servicio Universal de Telecomunicaciones (cuyo capítulo III establece los datos que deben figurar en las guías telefónicas incluidas en el ámbito del servicio universal, criterios para su elaboración, actualización y versión en formato electrónico) ha tratado la cuestión, diferenciando el supuesto de abonados al servicio telefónico fijo y de abonados a servicio de telefonía móvil.

Su apartado sexto al regular los datos que deben figurar en las guías telefónicas incluidas en el ámbito del servicio universal, incluida la versión en formato electrónico, indica en el punto segundo que «en las guías telefónicas figurarán los datos de los abonados del servicio telefónico fijo disponible al público que tengan asignado algún número y no hayan manifestado al operador del cual dependen dichos números su deseo de no aparecer en ellas, los datos de los abonados del servicio telefónico móvil que hayan solicitado a su proveedor del servicio su deseo de aparecer en ellas, acreditando fehacientemente la titularidad cuando no exista una relación contractual nominal, y los datos de los abonados que tengan asignados números de inteligencia de red que hayan solicitado al operador del cual dependen dichos números su deseo de figurar en ellas».

Se establece así, en el caso de abonados al servicio de telefonía móvil, la necesidad del consentimiento expreso de los mismos para poder incluir sus datos en guías telefónicas, consentimiento que no es necesario para la inclusión de los datos básicos de los abonados a servicios de telefonía fija.

En igual sentido, la más reciente Orden del Ministerio de Ciencia y Tecnología, de 26 de marzo de 2002, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado, después de efectuar la delimitación de los datos personales que podrán obtenerse a través de guías telefónicas y servicios de consulta telefónica en el apartado tercero, inserto en el Capítulo II que regula la gestión de datos personales de los abonados, aborda en el Capítulo III las condiciones de prestación de este segundo servicio, sometiendo tal actividad a la obtención de la autorización administrativa que se regula en el apartado quinto, estableciendo igualmente el principio de no discriminación por razón del operador a que se refieran los datos que debe regir dicha actividad así como la atribución de recursos de numeración para su prestación.

El punto tercero del apartado tercero de dicha Orden establece, en relación con los abonados a servicios de telefonía móvil, la distinción que ya se ha visto establecía la Orden de 21 diciembre de 2001, al indicar que «Se requerirá el consentimiento expreso de los abonados del servicio telefónico móvil disponible al público y de los abonados de los servicios de inteligencia de red para poder utilizar la información a la que se refiere el punto 1 de este apartado. Además, cuando los usuarios no sean titulares de un contrato de abono, tales como usuarios adicionales al titular del contrato, o propietarios de tarjetas de pago previo de servicios de telecomunicaciones, sólo se podrá utilizar dicha información cuando los interesados hayan manifestado su deseo de figurar en las guías o en los servicios de consulta sobre números de abonado. En el caso de usuarios adicionales al titular del contrato, se requerirá el consentimiento previo de éste».

Igualmente, en el apartado decimocuarto de la misma Orden, al referirse a los datos de abonados que los operadores deben facilitar a la Comisión del Mercado de las Telecomunicaciones en orden a permitir la prestación de servicios de directorio telefónico en régimen de libre concurrencia, se establece: «3. Además, los operadores comunicarán a la Comisión del Mercado de las Telecomunicaciones los abonados del servicio telefónico móvil disponible al público y los abonados de los servicios de inteligencia de red que hayan manifestado expresamente su deseo de figurar en las guías telefónicas o en los servicios de directorio.»

Puede así concluirse que, en razón de la delegación reglamentaria que establece la Ley General de Telecomunicaciones, se ha establecido en cuanto a los abonados a servicios de telefonía móvil la necesidad de exigir su consentimiento expreso para incluir sus datos básicos en guías telefónicas, lo cual a su vez resulta acorde con el régimen de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que resulta de los artículos 6 y 11 al regular el tratamiento y la cesión de datos de carácter personal.

2.2.11. Legislación aplicable a las misiones diplomáticas extranjeras en España

Se ha formulado una consulta referente a la aplicación de la LOPD a los ficheros de datos de carácter personal de que sean responsables las misiones diplomáticas extranjeras en España.

En primer lugar, hay que partir de lo dispuesto en el párrafo segundo del artículo 2.1 de la LOPD que, en relación con el ámbito territorial de aplicación de la Ley, establece que «se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito».

Las embajadas, como misiones diplomáticas de los estados en el extranjero, se constituyen como un conjunto de elementos sometidos al conocido como *«status»* diplomático, conjunto de privilegios e inmunidades que fruto de una larga evolución consuetudinaria, se encuentran actualmente codificados en la «Convención de Viena sobre relaciones diplomáticas», de 18 de abril de 1961, a la que España de adhirió el 21 de noviembre de 1967, que sustraen a la misión diplomática de la aplicación de determinadas disposiciones del ordenamiento jurídico del Estado receptor de las mismas. Así, entre las manifestaciones de dicho régimen se encuentran, entre otras, la inviolabilidad de los locales de la Misión (artículo 22), así como de sus archivos y documentos dondequiera que se hallen (artículo 24), la inviolabilidad penal e inmunidad jurisdiccional penal, civil —con algunas excepciones— y administrativa de los agentes diplomáticos (artículos 20 y 31).

Ello determina, conforme a su artículo 2. 1, de la Ley Orgánica 15/1999, una situación de extraterritorialidad de los ficheros o tratamientos de datos de carácter personal de que sean responsables dichas misiones diplomáticas extranjeras y se verifiquen por las mismas, los cuales se regirán a la postre por el derecho nacional del Estado que acredita la misión diplomática.

Dicho lo anterior, debe aclararse que las empresas españolas que puedan establecer relaciones con misiones diplomáticas extranjeras en España si estarán sometidas a la LOPD, y en concreto en los supuestos en que dichas relaciones jurídicas impliquen la comunicación o cesión de datos personales (por ejemplo, de sus empleados) que consten en ficheros o tratamientos de los que aquéllas sean responsables, debiendo en tal supuesto considerarse que

la comunicación de datos se estará efectuando al Estado del que la misión sea representante, y en consecuencia, se estará en presencia de una transferencia internacional de datos.

Con carácter general debe indicarse que las transferencias internacionales de datos se regulan en los artículos 33 y 34 de la Ley Orgánica 15/1.999, siendo definidas las mismas 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».

Tal Instrucción ha venido a fijar los criterios orientativos seguidos por la Agencia de Protección de Datos en la materia, aclarando a los interesados el procedimiento seguido por la Agencia de Protección de Datos para dar cumplimiento a las previsiones contenidas en la normativa reguladora de la materia.

Conforme a dicho régimen jurídico, las transferencias internacionales de datos efectuadas desde España están sometidas a la obtención de autorización del Director de la Agencia de Protección de Datos cuando las mismas se vayan a efectuar a países que no proporcionan un nivel de protección equivalente al de la LOPD y no concurra uno de los supuestos excepcionales previstos en el artículo 34 de la misma.

2.2.12. Aplicación del Reglamento de Medidas de Seguridad a los ficheros médicos

Se ha instado al Director de la Agencia de Protección de Datos por un Colegio Oficial de Médicos a dictar «un acto administrativo expreso en el que se establezca la no exigibilidad a los médicos, sujetos al secreto profesional, la obligación de adoptar las medidas de seguridad del Real Decreto 994/1999, con relación al tratamiento que efectúan de los datos relativos a la salud de sus pacientes, contenidos en las correspondiente historias clínicas».

Se fundamentó tal solicitud básicamente en la interpretación de que lo dispuesto en el Real Decreto citado no sería aplicable al ámbito médico, ya que a juicio del Colegio, la competencia para regular el tratamiento de los datos clínicos de los servicios sanitarios correspondería a las Comunidades Autónomas, no a una norma reglamentaria estatal.

El artículo 9 LOPD, dedicado a la seguridad de los datos, establece en su apartado tercero que «Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley».

En cumplimiento, entre otras, de esta remisión a desarrollo reglamentario, con fecha 11 de junio de 1999 se dictó el ya citado Real Decreto 994/1999, que aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo artículo 1 dispone que «El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal».

Derogada la LORTAD, la Ley Orgánica 15/1999 que la sustituyó declaró expresamente la vigencia de este Real Decreto, en lo que no se opusiera a la misma, en la Disposición Transitoria tercera.

En el ya tantas veces citado Reglamento de medidas de seguridad se establece en el artículo 4. 3, en lo que aquí interesa, que «Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de seguridad de nivel básico y medio, las calificadas como de nivel alto».

En relación con la alegación de falta de competencia del legislador estatal para regular esta materia ha de recordarse la distribución de competencias que en el concreto ámbito que nos ocupa establece la Constitución Española de 1.978, que atribuye la competencia, en lo que a la protección de los derechos fundamentales se refiere, al Estado. Así se desprende de lo dispuesto en su artículo 149.1 1º de aquélla, a cuyo tenor «el Estado tiene competencia exclusiva sobre la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes».

Por su parte, las Comunidades Autónomas deberán velar por el pleno desenvolvimiento de los derechos dentro del ámbito de sus respectivas competencias y de las condiciones que establezcan las normas del Estado reguladoras de dichos derechos fundamentales.

Dicho marco ha sido desarrollado por los artículos 41 y 42 de la LOPD, debiendo recordarse que el artículo 42.1 dispone que «Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento», añadiendo incluso el artículo 42.2 que «Si la Administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración».

Por último, algunas otras disposiciones de la Ley Orgánica se refieren a las competencias de las Autoridades de Control de las Comunidades Autónomas, siempre en el ámbito competencial diseñado por el artículo 41 de la Ley (esto es, en relación con los ficheros creados y gestionados por la propia Comunidad Autónoma o por las entidades integrantes de la Administración Local, dentro de su ámbito territorial). Así sucede en lo referente a la tutela de los derechos de acceso, rectificación, cancelación y oposición (artículo 18.2), en lo relativo a la inscripción de los códigos tipo, que podrán inscribirse en los registros autonómicos, sin perjuicio de la obligación de inscripción en el Registro general de Protección de Datos (artículo 32.3) o en lo atinente al ejercicio de la potestad de inspección (artículo 40.1), la potestad sancionadora en relación con los ficheros de titularidad pública (artículo 46) y la potestad de inmovilización de ficheros (artículo 49).

De todo lo antedicho se desprende que la Ley Orgánica 15/1999, de 13 de diciembre, vino a establecer un marco competencial fundamentalmente similar al ya diseñado por la anterior LORTAD, si bien que ampliando las competencias de las agencias autonómicas a los ficheros de los que sean responsables las entidades locales incluidas en su ámbito territorial, quedando las competencias de las citadas agencias limitadas a las expresamente establecidas en la Ley Orgánica, que han sido anteriormente enumeradas y exclusivamente en lo referente a los ficheros ya citados, sin que sea posible el ejercicio por las Comunidades Autónomas de ninguna competencia sobre los ficheros de titularidad privada ni sobre los de titularidad pública distinta de la Autonómica o local, aunque las competencias se desempeñen en el ámbito territorial de la Comunidad Autónoma (así, no cabrá el ejercicio de competencia alguna en relación con los ficheros de titularidad de los órganos integrantes de la Administración Periférica del Estado).

Por otra parte, y según se ha visto, la competencia para establecer el régimen legal en la materia de protección de datos corresponde al legislador estatal, por lo que la apreciación de que el legislador autonómico pueda establecer régimen específico o distinto en la materia no es acertada.

Debe, por todo ello, concluirse que el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio, es plenamente aplicable al tratamiento de datos de carácter personal relativos a la salud, cuando los mismos se contengan en ficheros automatizados, aun cuando dicho tratamiento se realice por personal médico sujeto al secreto profesional, sin que las especialidades que respecto al tratamiento de tales datos contienen los artículos 7. 6 y 8 de la LOPD establezcan o supongan excepción alguna al resto de obligaciones que establece dicha norma para los médicos que actúen como responsables de dichos ficheros o tratamientos, así como de las medidas de seguridad que establece aquél Reglamento, y sin que pueda considerarse que exista una extralimitación competencial del legislador estatal al establecer tal regulación.

A tal efecto, debe recordarse que la cuestión fue analizada detenidamente en la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, en cuyo fundamento jurídico 14 se indicaba: «la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10. 1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las comunidades autónomas ex art. 149. 1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías constitucionales».

Si bien la respuesta analizada fue emitida con anterioridad a la aprobación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo artículo 14.4 dispone que «Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental», debe entenderse que dicha disposición no impide en modo alguno alcanzar una conclusión similar a la analizada.

Ello se funda, primeramente, en que el artículo 17.6 de la propia Ley dispone que «Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal», lo que implica que las normas que a tal efecto se dictasen en el ámbito autonómico deberían en todo caso respetar el marco dispuesto por el legislador estatal en el Reglamento de Medidas de Seguridad, y en la interpretación del principio de aplicación uniforme de las normas de protección de datos en el territorio nacional, impuesto por la STC 290/2002 a la que se ha hecho anteriormente referencia.

2.2.13. Naturaleza de los ficheros colegiales

Diversos colegios profesionales han elevado consultas a la Agencia solicitando su parecer acerca de la naturaleza de los ficheros colegiales, en el sentido de considerarlos ficheros de titularidad pública o privada.

En relación con esta cuestión, debe señalarse que, si bien la LOPD delimita en su articulado el régimen de los ficheros de titularidad pública y privada, no establece un concepto de los mismos. Por esta razón, la delimitación deberá fundarse en los criterios que determinan la naturaleza jurídico-pública o jurídico-privada del responsable del fichero.

Esta conclusión se alcanza atendiendo a las peculiaridades establecidas para el régimen de los ficheros de titularidad pública, toda vez que los mismos únicamente podrían ser constituidos en caso de que se desarrollen como consecuencia del ejercicio de una competencia administrativa, tal y como se desprende del artículo 21.1 de la LOPD, que permite la cesión entre Administraciones Públicas cuando la misma se funde en el ejercicio de unas mismas competencias. En este mismo sentido, el artículo 20 de la Ley exige que los ficheros se encuentren relacionados con la actuación de una Administración con potestad para dictar la correspondiente Disposición de carácter general de creación del fichero.

Por tanto, se considera que la delimitación del régimen aplicable a los ficheros de titularidad pública y privada deberá fundarse en un doble criterio: por una parte el responsable del fichero deberá ser una Administración Pública y por otra, en los supuestos que pudieran plantear una mayor complejidad, sería necesario que el fichero sea creado como consecuencia del ejercicio de potestades públicas.

Dicho lo anterior, la delimitación de la naturaleza jurídica de las denominadas corporaciones de derecho público ha sido una cuestión ampliamente debatida por la doctrina administrativista, no habiéndose alcanzado en el momento presente una tesis unívoca sobre este particular.

No obstante, la jurisprudencia de nuestro Tribunal Constitucional ha analizado reiteradamente esta cuestión en numerosas sentencias, cuya cita conviene recordar en este momento.
En particular, merece especial atención la Sentencia 20/1988, cuyo Fundamento Jurídico cuarto analiza la naturaleza de los Colegios Profesionales, indicando lo siguiente:

> «Como ha declarado este Tribunal en anteriores ocasiones —SSTC 76/1983, de 5 de agosto; 23/1984, de 20 de febrero y 123/1987, de 15 de julio—, los Colegios Profesionales son corporaciones sectoriales que se constituyen para defender primordialmente los intereses privados de sus miembros, pero que también atienden a finalidades de interés público, en razón de las cuales se configuran legalmente como personas jurídico-públicas o Corporaciones de Derecho público cuyo origen, organización y funciones no dependen sólo de la voluntad de los asociados, sino también, y en primer término, de las determinaciones obligatorias del propio legislador, el cual, por lo general, les atribuye asimismo el ejercicio de funciones propias de las Administraciones territoriales o permite a estas últimas recabar la colaboración de aquéllas mediante delegaciones expresas de competencias administrativas, lo que sitúa a tales Corporaciones bajo la dependencia o tutela de las citadas Administraciones territoriales titulares de las funciones o competencias ejercidas por aquéllas».

Del mismo modo, la Sentencia 87/1989, recordando la doctrina sentada por la sentencia anteriormente transcrita, aclara, en su Fundamento Jurídico tercero que:

«Si bien es cierto que el carácter de Corporaciones Públicas que la Ley reconoce a los Colegios Profesionales no oscurece la naturaleza privada de sus fines y cometidos principales, también lo es que la dimensión pública de los entes colegiales les equipara a las Administraciones Públicas de carácter territorial, si bien tal equiparación quede limitada a los solos aspectos organizativos y competenciales en los que se concreta y singulariza la dimensión pública de los Colegios».

De lo indicado por el Tribunal en las dos sentencias transcritas cabe deducir una serie de consecuencias sumamente relevantes en la materia que nos ocupa.

Así, si bien es cierto que el Tribunal recuerda que los colegios profesionales son corporaciones sectoriales que se constituyen para defender primordialmente los intereses privados de sus miembros, pero que también atienden a finalidades de interés público, posteriormente esta afirmación se ve complementada por otras que, reiteradamente, atribuyen a los colegios una naturaleza jurídica que, incluso se indica, les equipara a las Administraciones Públicas de carácter territorial.

Así, se recuerda que dichas entidades ejercen en determinadas materias competencias administrativas, del mismo modo en que lo hacen las administraciones territoriales, lo que, precisamente sitúa a los Colegios bajo la dependencia o tutela de dichas Administraciones.

Del mismo modo, se indica que estas auténticas potestades administrativas, tales como la ordenación de la profesión colegiada o el ejercicio de la potestad sancionadora, entre otras, se ejercen por expresa atribución del propio legislador que, o bien atribuye expresamente la competencia a las entidades colegiales o le permite recabar la colaboración de las Administraciones territoriales mediante delegaciones expresas de competencias administrativas.

La misma conclusión se alcanzaría en caso de considerarse que la referencia a la «delegación» de las competencias ha de entenderse no en sentido estricto, sino que supusiera en la práctica una centralización o desconcentración de competencias, tal y como indican las Sentencias del Tribunal Supremo de 25 de octubre de 1993 (Ar. 1993\8010) y 17 de noviembre de 2001 (Ar. 2001\10273).

En consecuencia, a la luz de dicha sentencia, los colegios profesionales ejercen auténticas potestades de derecho público bien por expresa atribución del legislador bien por delegación o desconcentración a las mismas de dichas potestades.

De ello no cabe sino concluir que la naturaleza de los colegios profesionales es la de ente de derecho público equiparable, al menos en lo referente al ejercicio de las potestades administrativas que expresamente le atribuye el legislador, a las Administraciones

Públicas Territoriales. Ello se funda en el hecho de que, según se desprende de la jurisprudencia referenciada los colegios profesionales ejercen dichas competencias bien por expresa atribución del legislador, siendo así que la competencia originara para el ejercicio de potestades administrativas sólo puede encomendarse a Administraciones Públicas, bien por delegación o desconcentración de la Administración tutelante, dado que las mismas no podrían tener lugar a favor de quien no ostenta la naturaleza de Administración Pública.

Así se refleja en lo establecido en la propia normativa reguladora de los colegios profesionales.

En particular, el artículo 1.3 de la Ley 2/74, de 13 de febrero, reguladora de los Colegios Profesionales, si bien incluye entre los «fines esenciales de estas Corporaciones» la defensa de los intereses profesionales de los colegiados, debe recordarse que, con anterioridad a dicha finalidad incluye como esencial «la ordenación del ejercicio de las profesiones».

Como consecuencia de esta «finalidad esencial», evidentemente pública el artículo 5 atribuye a los Colegios las competencias para «ejercer cuantas funciones les sean encomendadas por la Administración» (apartado b), «ordenar en el ámbito de su competencia la actividad profesional de los colegiados, velando por la ética y dignidad profesional y el respeto debido a los derechos de los particulares y ejercer la facultad disciplinaria en el orden profesional y colegial» (apartado i), «adoptar las medidas conducentes a evitar el intrusismo profesional» (apartado l) o «cumplir y hacer cumplir a los colegiados las Leyes generales y especiales y los Estatutos profesionales y Reglamentos de Régimen interior, así como las normas y decisiones adoptadas por los órganos colegiados en materia de su competencia» (apartado u).

Al propio tiempo, los Colegios se someten a sus estatutos, que habrán de ser adoptados por la Administración Pública competente para ejercer la tutela sobre los mismos, bien la del Estado, bien las de las Comunidades Autónomas en cuanto a los colegios situados en su ámbito respectivo, en virtud de las correspondientes normas de traspaso de competencias.

Del mismo modo, la Ley 2/1974 establece en su artículo 8 que «los actos emanados de los órganos de los colegios profesionales y de los Consejos Generales en cuanto estén sujetos al Derecho Administrativo, una vez agotados los recursos corporativos serán directamente impugnables ante la Jurisdicción Contencioso-Administrativa».

De todo ello se desprende que los Colegios y Consejos se encuentran, al menos en parte de las funciones que desempeñan, sometidos al Derecho Administrativo, dictando auténticos actos administrativos revisables, como tales actos, por la jurisdicción contencioso-administrativa.

Al propio tiempo, el artículo 8.3 de la Ley 2/1974 enumera en su párrafo segundo las causas de nulidad de los actos administrativos dictados por los órganos colegiales, coincidiendo plenamente con lo previsto en la entonces vigente Ley de Procedimiento Administrativo, lo que no hace sino ahondar en la naturaleza pública de las potestades en cuya virtud se dictan dichos actos.

Además, la tesis que se ha venido indicando resulta asimismo confirmada por la jurisprudencia del Tribunal Supremo, bien por el hecho mismo de que su Sala Tercera ha venido ininterrumpidamente conociendo de los recursos planteados contra los actos dictados por los órganos de los Colegios, bien por el análisis efectuado por la Sala Primera cuando ante la misma se han planteado recursos de casación referentes a actos emanados de los órganos colegiales.

En este punto, y sin ánimo de resultar en exceso exhaustivos, la Sentencia de 28 de septiembre de 1998 (Ar. 1998\7289) recuerda en su único Fundamento de derecho que los Colegios Profesionales «tienen facultades de autoadministración sobre sus miembros y sus decisiones están sujetas al control jurisdiccional que es el contencioso-administrativo cuando se trata de defensa de la corporación, constitución de sus órganos, régimen electoral, decisiones sobre colegiación y disciplina, así como los actos de aprobación de presupuestos».

En el mismo sentido, la Sentencia del Alto Tribunal de 26 de noviembre de 1998 (Ar. 1998\8758), tras recordar la naturaleza dual de los Colegios Profesionales indica claramente que los mismos «desarrollan, a la par, una serie de actividades propias de un ámbito de derecho público, de servicio público e interés general, y otras de orden privado restringidas a su relación interna con los integrantes de las corporaciones y que carecen de toda eficacia externa o pública». Así reiterando la jurisprudencia citada, la sentencia concluye que «en los temas que versen, entre otros, sobre defensa de la corporación, constitución de sus órganos, régimen electoral, decisiones sobre colegiación y disciplina, por su evidente matiz de derecho público, (los Colegios) están sujetos al control jurisdiccional del orden contencioso-administrativo».

En resumen, los colegios profesionales, en cuanto dicten actos relacionados, entre otros, con las materias reseñadas por la jurisprudencia, ejercen auténticas potestades administrativas, siendo tales decisiones auténticos actos administrativos.

La consecuencia de todo lo que se ha venido indicando, aplicando lo dispuesto en la LOPD, es que los ficheros creados o gestionados por los Colegios Profesionales o sus Consejos para el ejercicio de las potestades a las que se ha venido haciendo referencia se encontrarán sometidos al régimen de los ficheros de titularidad pública, contenido en los artículos 20 y siguientes de la Ley Orgánica.

En este sentido, es necesario recalcar que, del tenor de la Ley, y en especial de su artículo 21, la naturaleza pública de los ficheros viene expresamente ligada a la titularidad y ejercicio de competencias de derecho público. Sólo de este modo podría resultar comprensible y aplicable la referencia efectuada por dicho precepto a la comunicación de los datos «para el ejercicio de competencias» diferentes o que versen sobre materias distintas.

Del mismo modo, teniendo en cuenta que la Ley 2/1974 atribuye a los Colegios Profesionales el ejercicio de la potestad disciplinaria, de derecho público sobre sus colegiados, la consideración de los ficheros de dichas Corporaciones como de titularidad privada haría imposible la creación de ficheros referentes al ejercicio de esta potestad, toda vez que el artículo 7.5 de la Ley Orgánica 15/1999 limita claramente la creación de estos ficheros al disponer que «los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras».

Todo ello no hace sino reincidir en nuestra tesis de que los ficheros de que sean responsables los Colegios Profesionales y Consejos Generales, en cuanto se relacionen con el ejercicio por los mismos de sus competencias de derecho público y, en consecuencia, con la atribución a los mismos de potestades administrativas, se encontrarán sometidos al régimen de los ficheros de titularidad pública y no al de los ficheros de titularidad privada, que será aplicable a los ficheros no vinculados con el ejercicio de tales potestades.

2.2.14. Ejercicio del derecho de acceso por los herederos del afectado

Se ha planteado si resulta posible que los herederos de una persona fallecida ejerciten el derecho de acceso a los datos de la misma o si es posible que alguno de ellos pueda obstaculizar dicho acceso.

La resolución de la cuestión planteada deberá obtenerse en función de la naturaleza misma del derecho protegido por la norma, lo que conduce a la necesidad de determinar si la muerte de las personas da lugar a la extinción del derecho a la protección de la «privacidad» o a la denominada «libertad informática», regulada por la LOPD, ya que el artículo 32 del Código Civil dispone que «la personalidad civil se extingue por la muerte de las personas», lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

La protección otorgada por la Ley frente a las intromisiones que supongan una vulneración de los derechos al honor y a la intimidad subsiste con posterioridad a la muerte de las personas. En ese sentido, cabe destacar que la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas

que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

Por su parte, la Ley Orgánica 15/1999 tiene como objeto esencial, tal y como dispone su artículo 1, la protección de los derechos fundamentales y, en especial del honor y la intimidad frente al tratamiento de los datos de carácter personal, estableciendo a lo largo de su articulado las medidas precisas para asegurar que dicha protección se lleva plenamente a efecto.

Del análisis conjunto de las disposiciones contenidas en ambas Leyes se desprende que la legitimación conferida para el ejercicio de las acciones reconocidas en la Ley Orgánica 1/1982 existirá, en el ámbito de la LOPD, cuando la actuación de las personas legitimadas tenga por directo y exclusivo objeto el ejercicio de las acciones tendentes a la protección del honor, la intimidad personal y familiar y la propia imagen de las personas fallecidas, no siendo posible la actuación de éstas en cualquier otro supuesto en que la finalidad de su actividad difiera de la antedicha protección.

Ello supone que, las personas legitimadas por la Ley Orgánica 1/1982 carecerán de legitimación para el ejercicio de los derechos reconocidos por la LOPD, salvo en los supuestos en que esos derechos se ejerciten como instrumento para la realización de alguna de las finalidades protectoras indicadas que la Ley les atribuye. Fuera de estos supuestos no será posible entender que la actividad de los herederos o personas referidas en el artículo 4 de la Ley Orgánica 1/1982 se encuentra amparada por la LOPD.

No obstante, sería posible el acceso de los herederos a los datos del causante siempre que los mismos aparezcan directamente relacionados con su propia condición de heredero (por ejemplo, el acceso a los datos necesarios para conocer el caudal relicto o el estado de determinados bienes de la herencia). Sin embargo, el acceso a la información a la que nos referimos no podría entenderse relacionado con el derecho de acceso consagrado en la legislación de protección de datos de carácter personal, sino que se desprendería del derecho de todo heredero a conocer el caudal relicto y el estado del mismo, así como realizar las acciones necesarias para su determinación y defensa, toda vez que el mismo sucede al causante en todos sus derechos y obligaciones como consecuencia de su muerte, tal y como determinan los artículos 651, 659 y 661 del Código Civil.

En consecuencia, a la vista de lo que se ha venido exponiendo, los herederos podrán tener acceso a los datos del causante en cuanto ello suponga el ejercicio en su nombre de una acción amparada por la Ley Orgánica 1/1982 o en cuanto dicho acceso se produzca en defensa de su derecho hereditario. Sin embargo, tales accesos no podrán ser considerados como manifestaciones del derecho de acceso, consagrado por el artículo 15 de la LOPD.

2.2.15. Acceso a datos catastrales

Se ha planteado una consulta relacionada con lo establecido en la Disposición Adicional Segunda de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, que vino a regular el Acceso a los datos catastrales.

Dicha disposición establece en su apartado primero que «Todos podrán acceder a la información de los inmuebles de su titularidad y a la información de datos no protegidos contenida en el Catastro», añadiendo que «Tienen la consideración de datos protegidos el nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren inscritos en el Catastro como titulares o sujetos pasivos del Impuesto sobre Bienes Inmuebles, así como el valor catastral y los valores del suelo y, en su caso, de la construcción, de los bienes inmuebles individualizados».

Analizando dicha disposición legal, puede indicarse que la misma se ajusta al régimen general de cesión de datos de carácter personal que establece el artículo 11. 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 objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones del cedente y del cesionario con el previo consentimiento del interesado».

Debe considerarse por otro lado que tal disposición sí permite en determinados supuestos de interés legítimo, el acceso inconsentido a los datos de identidad del titular, como en casos de identificación de parcelas colindantes, sucesiones mortis causa, titularidades de derechos reales, etc. Por tanto, la posible contradicción que pudiera alegarse, al considerar que puede accederse a los datos en casos de interés legítimo, no es tal, puesto que como se ha indicado, la disposición delimita expresamente qué supuestos de interés legítimo justifican tal posibilidad ni abarcar cualquier supuesto de interés legítimo, sin existir en consecuencia esa contradicción.

Fuera de tales casos, existen otros registros públicos inmobiliarios, como el Registro de la Propiedad, que entre sus principios básicos cuentan con el de publicidad formal, siendo en consecuencia un registro idóneo para acoger otros supuestos de interés legítimo en el conocimiento de titularidades inmobiliarias.

Por todo ello, puede concluirse que la disposición normativa objeto de consulta no resulta contradictoria con las normas contenidas en la LOPD y que debe interpretarse en sus propios términos, siendo plenamente respetuosa con la misma, atendiendo a la específica finalidad del Catastro como registro administrativo vinculado u orientado a la gestión tributaria de entidades locales (artículo 77 de la Ley 39/1988, de 28 de Diciembre, de Haciendas Locales), sin perjuicio de que por disposición legal tenga en ciertos casos otros posibles usos.

3. Análisis Jurisprudencial

3.1. Análisis de las principales sentencias de la Jurisdicción Contencioso Administrativa

Según dispone el artículo 48.2 de la LOPD, que reproduce lo que ya establecía el artículo 48.2 de la derogada LORTAD, las resoluciones del Director de la Agencia de Protección de Datos ponen fin a la vía administrativa. Por ello, y sin perjuicio de la eventual interposición del recurso potestativo de reposición (al que se refiere el artículo 116 Ley 30/1992), dichas resoluciones sólo serán susceptibles de impugnación en vía contencioso-administrativa.

En este orden jurisdiccional, los órganos fiscalizadores competentes durante el año 2002 han sido las Salas de lo Contencioso-administrativo tanto de los Tribunales Superiores de Justicia como de la Audiencia Nacional, tomando en cuenta que el recurso hubiera sido interpuesto, respectivamente, antes de la entrada en vigor de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa, que atribuyó a la Audiencia Nacional la competencia anteriormente radicada en los tribunales Superiores de Justicia. Además, como dato novedoso frente a lo indicado en la Memoria del año anterior, durante el año 2002 han comenzado a notificase a la Agencia Sentencias dictadas por el Tribunal Supremo, que resuelven recursos de casación interpuestos contra las sentencias dictadas por los Órganos jurisdiccionales a los que se acaba de hacer referencia, en los casos en que así lo permite la Ley Rituaria.

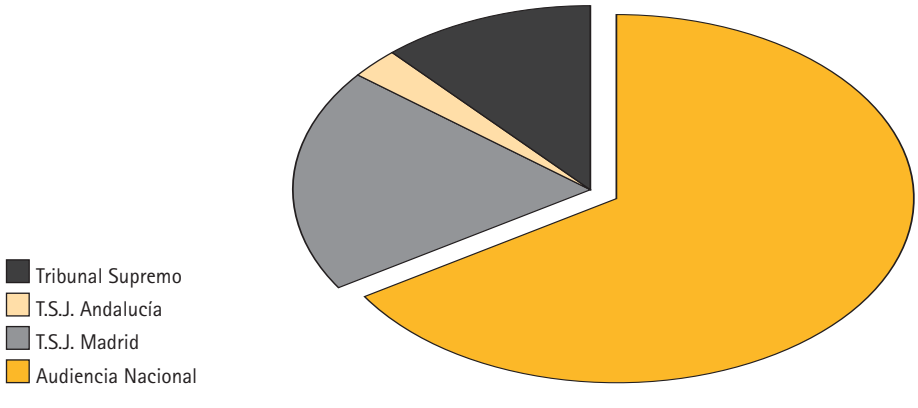
Hasta la fecha en que se redacta la Memoria de la APD correspondiente a 2002, se tiene conocimiento de un total de 99 Sentencias dictadas por las Salas de los Tribunales Superiores de Justicia y la Audiencia Nacional, conociendo recursos interpuestos en primera o única instancia, y 11 Sentencias dictadas por el Tribunal Supremo, resolviendo recursos de casación o casación para unificación de doctrina, así como dos Autos del Alto Tribunal por los que se declara la inadmisión de sendos recursos de casación interpuestos contra sentencias del Tribunal Superior de Justicia de Madrid que confirmaban la resolución dictada por la Agencia.

De las 99 sentencias dictadas en primera o única instancia 74 lo fueron por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional; 22 por la Sala del mismo Orden del Tribunal Superior de Justicia de Madrid, y 3 por la del Tribunal Superior de Justicia de Andalucía. Como puede comprobarse, cada vez es mayor la proporción de las sentencias dictadas por la Audiencia Nacional, dado que los recursos pendientes en las Salas de los Tribunales Superiores de Justicia son cada vez menores.

El cada vez mayor número de las sentencias procedentes de la Audiencia Nacional y Tribunales Superiores de Justicia 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 Supremo.

El siguiente gráfico muestra la distribución de las sentencias, teniendo en cuenta el Órgano que ha dictado las mismas

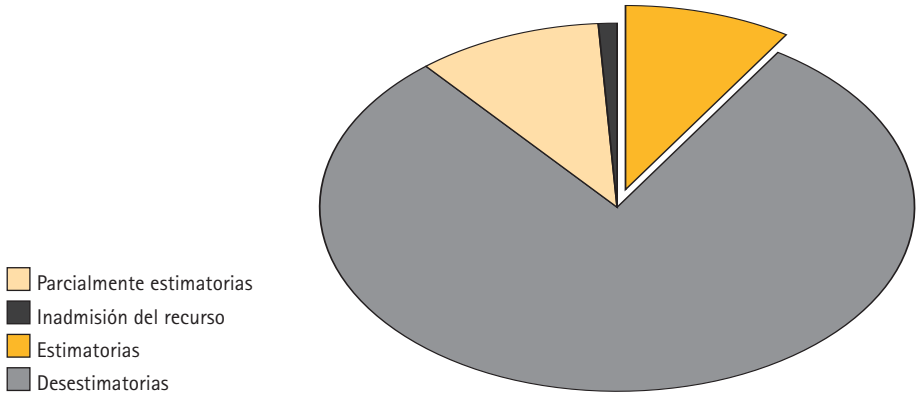
SENTENCIAS POR ÓRGANO JURISDICCIONAL



En cuanto al fallo de los pronunciamientos judiciales, debe indicarse que de las 99 sentencias dictadas en primera o única instancia, 79 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia, que quedaron plenamente confirmadas, 10 estimaron par-

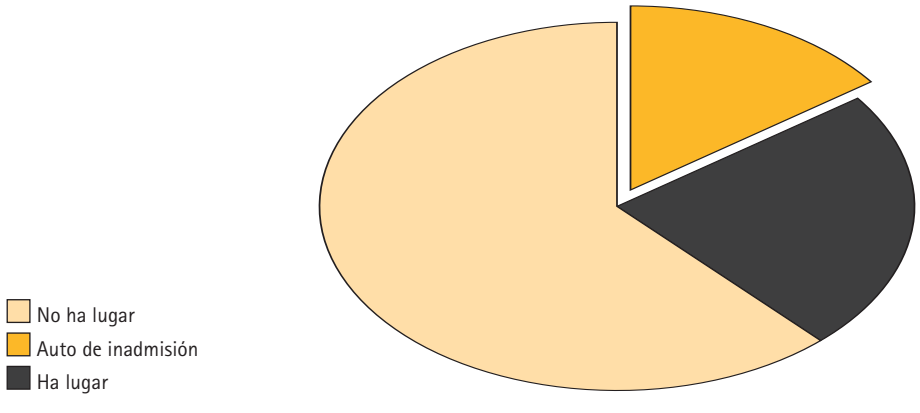
cialmente los recursos, mientras que solamente 9 de ellas estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia. En un único caso se inadmitió el recurso.

SENTENCIAS EN PRIMERA O ÚNICA INSTANCIA



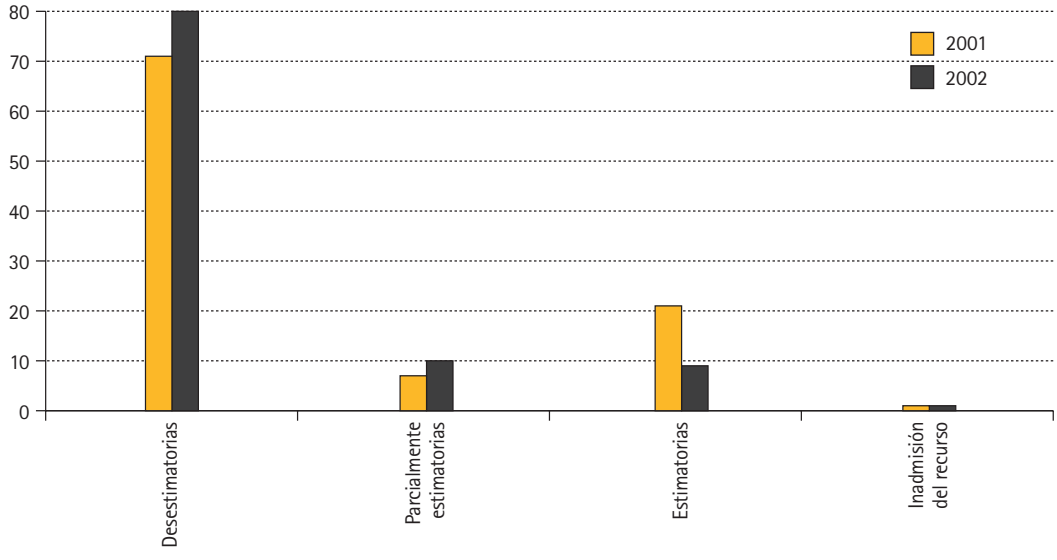
De las sentencias dictadas por el Tribunal Supremo, ocho declararon no haber lugar al recurso interpuesto y tres de ellas declararon haber lugar al mismo.

RESOLUCIONES DEL TRIBUNAL SUPREMO



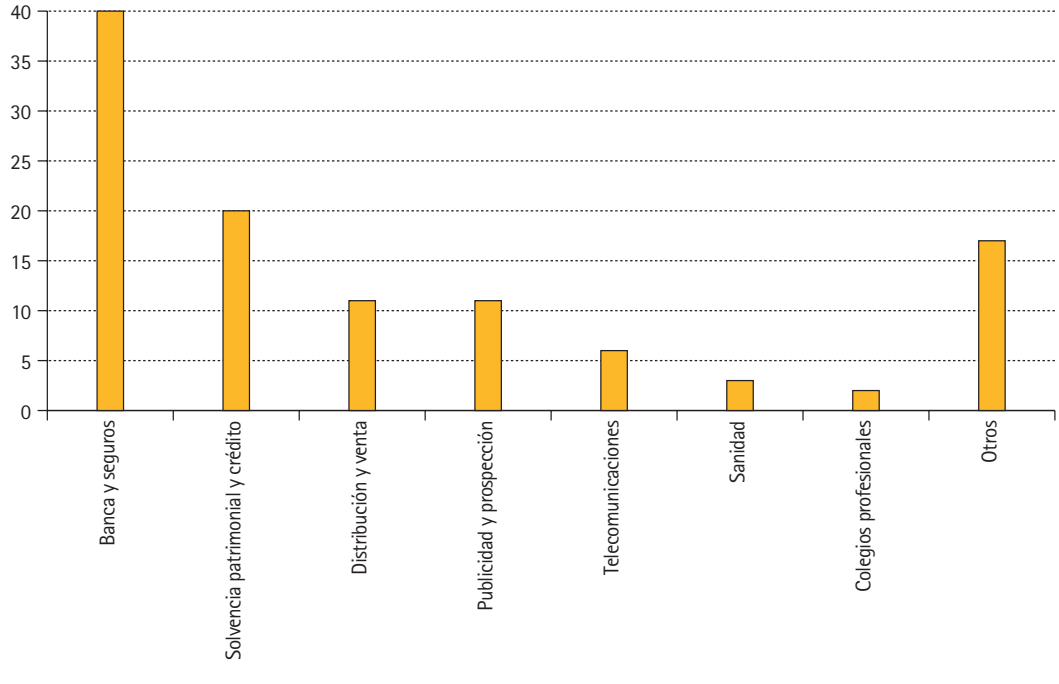
Como puede comprobarse, la cifra referente a los recursos en que el criterio de la Agencia ha sido confirmado en sede jurisdiccional es creciente, alcanzando en el año 2002 un 80 por 100 de las sentencias dictadas en primera o única instancia. Además, como dato aún más relevante, el porcentaje de sentencias estimatorias de los recursos ha descendido en el año 2002 a un 9 por 100 del total, frente al 21 por 100 del año 2001. En consecuencia, los criterios de la Agencia son considerados en la inmensa mayoría de los casos como ajustados a derecho por parte de quienes tienen la misión de enjuiciarlos. Así puede comprobarse en el siguiente gráfico:

COMPARATIVA POR FALLO (PORCENTAJES)



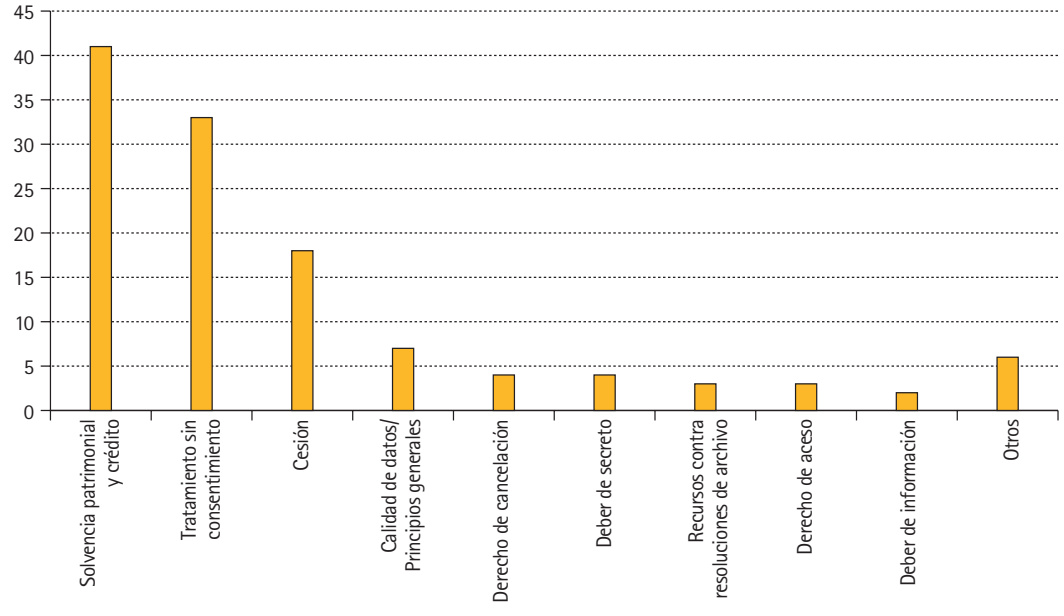
Atendiendo al sector o ámbito de actividad al que pertenece el recurrente, puede comprobarse en el siguiente gráfico cómo se mantienen los ya recogidos en anteriores memorias, con un amplio predominio del sector bancario y del de solvencia patrimonial y crédito:

SECTOR AL QUE PERTENECE EL RECURRENTE



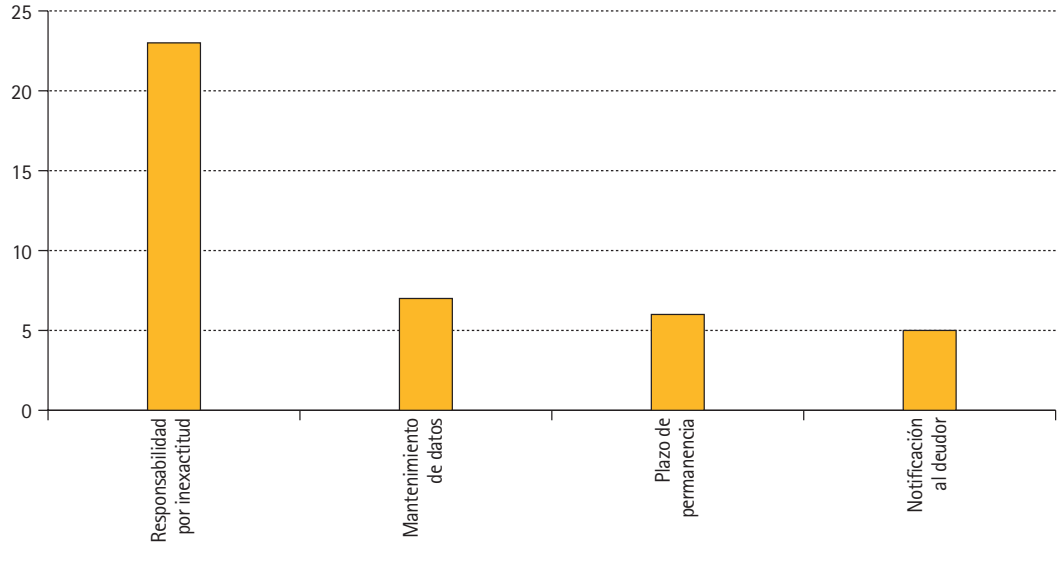
En cuanto a las materias, dentro del ámbito de la protección de datos, a las que se refería el proceso cabe también extraer una conclusión de continuidad similar a la referente al sector de actividad del recurrente. Así resulta de la siguiente distribución:

SENTENCIAS POR MATERIAS



Al igual que en los años 2000 y 2001, en este periodo el mayor número de sentencias ha guardado relación con 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, en las que se aprecia una mayor incidencia de las cuestiones relacionadas con la responsabilidad en caso de inclusión de datos inexactos o indebidos en los ficheros, que acaparan casi un 60 por 100 del total:

SENTENCIAS SOBRE FICHEROS DE SOLVENCIAS



3.2. Sentencias de mayor relevancia dictadas en primera o única instancia

3.2.1. Conservación de datos de obligaciones satisfechas en ficheros de solvencia patrimonial y crédito. Saldo cero

La Sentencia de la Sala de lo Contencioso-administrativo de la Audiencia Nacional de 10 de mayo de 2002 vino a resolver el recurso planteado contra resolución de la Agencia de 1 de marzo de 2001, por la que se sancionaba a una determinada entidad informante de un fichero de solvencia patrimonial y crédito relacionado con el cumplimiento de obligaciones dinerarias por no haber instado la cancelación de los datos referidos a una deuda efectivamente satisfecha cinco años antes del momento en que se formuló la denuncia. En el fichero común constaba la existencia de dicha obligación, aunque con saldo cero.

La Sentencia desestima el recurso y confirma el criterio sustentado por la Agencia, razonando que dicha conducta, conforme a lo establecido en la derogada LORTAD, es contraria a lo dispuesto en la LOPD, cuyo artículo 4.3 dispone que «Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado», reemplazando así el requisito de que el dato responda a la situación «real» del afectado por el de que responda a la situación «actual» del mismo. En el mismo sentido, se recuerda que una reforma similar se ha producido en el artículo 29.4 de la LOPD, a cuyo tenor «Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos».

Así, el Fundamento de Derecho cuarto de la Sentencia recuerda que «el reflejo del dato personal «saldo 0» no es un reflejo veraz de la situación real del afectado, puesto que el denunciante no tenía saldo alguno al haberse cancelado la deuda, por lo que la única razón que explica la permanencia del dato en un fichero de solvencia patrimonial, cuando la deuda ha sido cancelada, es informar sobre la morosidad reciente, pero pasada, del afectado, lo que no se conjuga con la previsión del artículo 4.3 de tanta cita que impone que se refleje la situación actual del afectado, es decir, su solvencia en la actualidad».

Prosigue la Sentencia indicando que «la única finalidad que tiene el mantenimiento en un registro de solvencia patrimonial, a instancias de la entidad informante y ahora recurrente, de los datos de quien no tiene deudas, con el término «saldo 0», es informar de su morosidad anterior, recordar sus deudas pasadas, lo que resulta incompatible con la situación «actual» del afectado, que establece el artículo 4.3 de la Ley Orgánica».

Al propio tiempo, se añade en el Fundamento de derecho sexto que «la inclusión en este tipo de ficheros se hace de modo diferente, como excepción a la regla general de prestación de consentimiento del afectado (...) este mecanismo excepcional de acceso de los datos de carácter personal a este tipo de ficheros, cuando además, resultan afectados los derechos fundamentales, impiden interpretar el tipo sancionador de forma diferente a la anteriormente referida», concluyendo que «la función que cumplen estos ficheros no puede imponerse por encima de la salvaguardia de los derechos fundamentales y de las previsiones plasmadas en la Ley en forma de tipos sancionadores».

3.2.2. Cesión de datos para la prestación de nuevos servicios no solicitados por el afectado

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 13 de septiembre de 2002 desestima el recurso interpuesto contra resolución de la Agencia de 8 de diciembre de 2000.

Los hechos pueden ser resumidos del siguiente modo: en agosto de 1995 la afectada contrató una póliza de seguro para su vehículo con una determinada entidad aseguradora. Un año después dicha aseguradora contrató con una entidad expedidora de tarjetas de crédito para el uso de combustible un contrato por el que se facilitaría a sus asegurados este tipo de tarjeta, comprometiéndose la entidad a asumir el riesgo de la tarjeta siempre que se disponga de los datos del cliente y que el mismo no se encuentre incluido en determinados ficheros de solvencia patrimonial y crédito. De este modo, sin que la afectada hubiera en ningún momento solicitado la tarjeta ni prestado su consentimiento al tratamiento efectuado por la entidad expedidora, fue creada una tarjeta a su nombre que nunca fue recibida por la afectada sino por un tercero que hizo uso de la misma por importe cercano al millón de pesetas. La entidad expedidora anotó el descubierto en la cuenta de la afectada, que denunció los hechos como estafa, siendo descubierto el tenedor de la tarjeta.

El recurso analizado fue interpuesto por la entidad gestora de la tarjeta de crédito, alegando que la misma era un mero encargado del tratamiento, por lo que no se precisaba el consentimiento de la afectada para crear dicha tarjeta, conforme a lo dispuesto en el artículo 27 de la LORTAD, entonces vigente, y que, en todo caso se contaba con su consentimiento tácito al tratamiento.

La sentencia razona la inexistencia de la condición de encargado del tratamiento en la recurrente, señalando que, si bien es cierto que entre la misma y la aseguradora existe una relación de prestación de servicios, dicha relación incorpora ciertas especialidades (a la vista del contrato suscrito por ambas) que la hacen singular, dado que la entidad gestora es quien asume el riesgo de la emisión de la tarjeta, encargándose por ello de analizar los

riesgos de cada titular antes de la expedición, comprobando la inclusión de sus datos en los ficheros de morosos.

De este modo, se señala en el Fundamento de Derecho quinto de la sentencia que «la denunciante se encuentra con un desfalco en una tarjeta que no ha solicitado y nunca ha usado y debe responder ante (la recurrente) con quien no le une relación alguna y ante la que no ha prestado ningún consentimiento para la emisión de la tarjeta (...) obligaciones que el deudor ha de cumplir sin haber mostrado voluntad alguna de contraerlas». Añade la Sentencia que del contrato suscrito entre la recurrente y la aseguradora se deriva «la creación de una nueva relación jurídica con las personas cuyos datos ha cedido (la aseguradora) que es de todo punto incompatible con la relación de servicios por cuenta de otro».

Así se concluye que «lo importante y trascendente es que a quien no había solicitado el uso de una tarjeta de crédito se le extendiera con unos datos que ella había proporcionado para otra finalidad», concluyéndose que «en ningún caso ha existido consentimiento tácito o subsiguiente por parte de (la afectada) que nunca tuvo conocimiento de la existencia de la misma hasta que pudo comprobar un descubierto en su cuenta bancaria por un importe de 934.128 pts. Y nunca la tuvo en su poder».

Por último, la sentencia incide en el grado de culpabilidad exigible para la imposición de la sanción, señalando que «basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia para evitar, como en el caso que nos ocupa, un tratamiento de datos personales sin consentimiento de la persona afectada, lo que denota una falta evidente en la observancia de estos deberes que conculcan claramente los principios y garantías establecidas (...) concretamente el del consentimiento del afectado».

Este criterio fue ratificado por la propia Sala en Sentencia de 20 de septiembre de 2002, que resuelve el recurso interpuesto por la entidad aseguradora, a la que la Agencia había sancionado por vulneración del artículo 11 de la LOPD.

3.2.3. Requisitos para la existencia de un encargado del tratamiento. Prestación de servicios de «scoring»

La Audiencia Nacional se ha pronunciado en tres ocasiones en relación con la prestación por una determinada entidad de servicios de *«scoring»* o valoración de la situación financiera de los clientes de una tercera que contrata la prestación de dichos servicios. Así cabe citar las sentencias de 18 de enero, 14 de junio y 15 de noviembre de 2002, siendo la resolución en todos los casos confirmatoria de la resolución dictada por la Agencia y, en consecuencia, desestimatoria del recurso.

En la primera y la tercera de las sentencias anteriormente citadas se confirma el criterio de la Agencia, que consideró esta práctica una cesión sin consentimiento del afectado, al no constar prueba alguna que acreditara la existencia de un contrato escrito entre la entidad solicitante y la que efectuó los servicios de *«scoring»* y no haberse recabado el consentimiento del afectado para la realización del mismo.

En resumen, esta práctica puede resumirse como la comunicación por parte de una empresa, generalmente prestadora de servicios a sus clientes de los datos de aquéllos a una tercera empresa, generalmente perteneciente al sector del estudio de la solvencia patrimonial y crédito, a fin de que por la misma se considere a dichos clientes «aptos» o «no aptos», en función bien de los datos facilitados, bien de los que la propia destinataria tiene en su poder.

La Sentencia de 15 de noviembre de 2002 analiza si, al amparo del artículo 27 de la LORTAD, vigente al tiempo de producirse los hechos, resulta necesaria la forma escrita en el contrato a celebrar entre la entidad solicitante de los servicios de *«scoring»* y la que presta dichos servicios para que dicha práctica pueda ser considerada amparada por la regulación que dicha Ley efectuaba de la prestación de servicios por cuenta de terceros, actualmente regulada por el artículo 12 de la LOPD.

Dicha sentencia considera que sería necesaria la celebración del contrato en forma escrita por los siguientes motivos:

- Porque así se infiere de una interpretación literal de la norma.

- Porque tal interpretación resulta más acorde con la finalidad de la Ley, dado que si bien no existe una cesión en sentido estricto, se produce una transmisión de los datos que supone un peligro o riesgo de publicidad del dato, que se encuentra en poder de un tercero distinto de aquél a quien el afectado consintió el tratamiento, exigiendo el legislador al responsable un deber de diligencia en la elección del encargado del tratamiento, que garantice la integridad de los derechos del afectado, exigiendo la operatividad de esta finalidad que el contrato sea escrito y con las menciones previstas en la Ley, pues «en otro caso se generaría una inseguridad jurídica en perjuicio del titular del dato».

- Porque la exigencia de constancia escrita se deriva del artículo17.2 de la Directiva 95/46/CE, que dispone que «la realización de tratamiento por encargo deberá estar regulada por un contrato o acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento», precepto que, añade la Sentencia «la doctrina interpreta en el sentido de que es preciso un contrato escrito y queda corroborada por el actual artículo 12 de la LOPD que habla expresamente de constancia por escrito».

En relación con el régimen establecido en la LOPD la sentencia ofrece asimismo una interpretación de dicho precepto que resulta sumamente relevante a los efectos de su aplicación futura, al señalar en su Fundamento de Derecho cuarto que «ciertamente el artículo 12 de la Ley también habla de constancia en alguna otra forma» que permita acreditar la celebración del contrato. Pero estos términos no pueden interpretarse, como pretende la recurrente, en el sentido de que rige el principio de libertad de forma y es posible un pacto verbal, lo que sería contradictorio con que al mismo tiempo la norma exija forma escrita. Lejos de ello lo que ocurre es que existen formas de formalización que pueden ofrecer garantías similares a la forma escrita (Vgr. un supuesto de firma electrónica avanzada conforme a lo establecido en el Real Decreto-Ley 14/1999, caso en el que no existiría un documento escrito en sentido estricto).

Al propio tiempo, considerada ya por la sentencia la existencia de una cesión de datos, se señala que la misma no cuenta con el consentimiento del afectado, dado que las cláusulas incluidas en el contrato entre la prestadora de servicios al afectado y aquél no hacían en ningún lugar mención de la posible cesión de sus datos para «valorar la aptitud crediticia de sus titulares, ni en ella se recaba el consentimiento de éstos para que sus datos puedan ser cedidos a terceros con dicha finalidad».

3.2.4. Vulneración del deber de seguridad. Documentación no destruida.

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia nacional de Madrid de 13 de junio de 2002 desestima el recurso interpuesto contra Resolución de la Agencia de 21 de mayo de 2001, de la que se dio cuenta en la Memoria correspondiente al anterior ejercicio, en que se sancionaba a una determinada entidad por vulneración del deber de implantar las medidas de seguridad exigidas por la LOPD y el Reglamento de Medidas de Seguridad, como consecuencia del hecho de haber aparecido en contenedores de basura documentos de uso interno de la entidad que contenían datos de carácter personal. Este hecho además alcanzó relevancia pública al aparecer esta noticia reflejada en distintos medios de comunicación.

La sentencia, tras considerar adecuado el criterio de la Agencia que, tras considerar los hechos como contrarios tanto al artículo 9 de la LOPD (deber de seguridad) como al artículo 10 de la misma (deber de secreto), se limitó a sancionarlos por la primera de las vulneraciones al considerar que la segunda infracción quedaba automática e inexorablemente subsumida en la primera, declara improcedentes las alegaciones de la entidad recurrente, que consideraba la inexistencia de infracción, al haberse adoptado por aquélla las adecuadas medidas y aprobado el correspondiente documento de seguridad, al tiempo que se consideraba vulnerada la presunción de inocencia, por no haberse acreditado efectivamente que los documentos hallados procedieran inequívocamente de sus oficinas.

Así, en relación con la primera de las alegaciones, la sentencia señala que «no basta con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto (art. 9 LOPD). Y por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados (...) la observancia de aquellas instrucciones».

Continúa la sentencia señalando que en el presente caso la recurrente «no prestó la diligencia necesaria en orden a la efectiva observancia de aquellas medidas de seguridad, pues de otro modo no se explica que los documentos en los que figuran datos de carácter personal apareciesen publicados en una revista de amplia difusión en la que se afirmaba que habían sido encontrados en la basura», recordando que la resolución sólo sancionaba a la entidad por la aparición de listados de datos de carácter personal que además procedía de documentos de uso estrictamente interno de la entidad.

Precisamente por este motivo, la sentencia declara no haber lugar a ninguna vulneración del principio de presunción de inocencia, dado que «ha quedado acreditado, siquiera sea por exclusión de otra explicación razonable, que la conducta que se sanciona es imputable a la entidad (...) ahora demandante».

3.2.5. Tratamiento de datos médicos para el control del absentismo

Las sentencias de la Audiencia Nacional de 12 de abril y 10 de mayo de 2002 desestiman dos recursos frente a resoluciones de la Agencia que guardan una enorme semejanza.

En ambos casos, la resolución recurrida había sancionado por tratamiento de datos relacionados con la salud de las personas a sendas empresas que prestaban para un Órgano de una Administración Pública, en el primero de los casos, y una Entidad Pública Empresarial, en el segundo, un servicio consistente en el control del absentismo de sus empleados. Para ello, el empleador facilitaba a las entidades los datos de sus trabajadores, incluyendo las fechas de alta y baja, en su caso, y el personal médico de las entidades sancionadas visitaba a esas personas, elaborando un informe médico en que se recogía el diagnóstico de la enfermedad que padecía el trabajador; esos informes eran almacenados en los ordenadores de la entidad sin contar con el consentimiento del afectado.

En ambos casos, el contrato celebrado indicaba como finalidad del mismo «el control del absentismo»; con cita expresa en uno de ellos del artículo 20.4 del Estatuto de los Trabajadores, que atribuye al empresario la facultad de verificar el estado de enfermedad o acci-

dente del trabajador que sea alegado para justificar sus faltas de asistencia al trabajo, mediante el reconocimiento a cargo de personal médico.

Por su parte, las entidades recurrentes fundaban la licitud del tratamiento en lo establecido en el párrafo primero del artículo 7.6 de la LOPD, a cuyo tenor «No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto».

Frente a ello, las sentencias recuerdan que la aplicabilidad de dicho precepto sólo resulta posible cuando el tratamiento se efectúa realmente para «la prevención y el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios», indicando que, según la primera de las citadas «en nuestro caso, el tratamiento de datos personales relativos a la salud efectuada por la entidad recurrente, no se realizaron con esa finalidad, sino en virtud de un contrato suscrito con (...), cuyo objeto era controlar el absentismo del personal que prestaba sus servicios en (...). Y para ello (la recurrente) crea un fichero en el que registra los datos de diagnóstico médico de cada trabajador que utiliza como medio para elaborar un informe que remitirá a (...), para que éste pueda controlar el absentismo laboral».

Prosigue la sentencia en su Fundamento de Derecho V que «la prestación del servicio médico realizado por los facultativos (...) no tiene por objeto ni la mejora, ni la prevención de la salud de las personas a quienes examina y cuyos datos incorpora al fichero, es decir, no realiza una prestación necesaria para su salud, ni tampoco para el tratamiento médico a que pudieran estar sometidos, ni para la investigación científica o el desarrollo de la medicina, sino que la prestación únicamente está al servicio de los intereses del arrendador que, a través de ese mecanismo, pretende evitar el absentismo en el trabajo».

«Por tanto —concluye la sentencia— no puede hablarse de prestación de servicios médicos en los términos exigidos en la Ley, y ello aunque intervengan facultativos sometidos al secreto profesional, sino de otro tipo de prestación de servicios, no amparada en el artículo 7.6 de la LOPD, para cuyo tratamiento informatizado de datos precisa el consentimiento del afectado».

3.2.6. Tratamiento de datos de profesionales sin su consentimiento para su inclusión en una publicación periódica

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 21 de noviembre de 2002 confirma la resolución de la Agencia de 18 de mayo de 2000 en que

es sancionada una determinada empresa editora de una publicación relacionada con el mundo de la arquitectura por tratamiento de datos personales de diversos profesionales de ese sector sin contar con su consentimiento. Dicha resolución ponía fin al procedimiento iniciado como consecuencia de la denuncia de 48 de los profesionales cuyos datos constaban en dos números de la revista, al no haberse podido acreditar por la recurrente que los datos procedieran de fuentes accesibles al público.

La sentencia analizada resulta sumamente interesante en cuanto delimita claramente si las previsiones de la LORTAD (y hoy de la LOPD) resultan de aplicación a los profesionales, por un lado y, por otro, en cuanto establece a quién corresponde la carga de la prueba de que los datos sometidos a tratamiento proceden de fuentes accesibles al público.

En cuanto a la primera de las cuestiones, la Sentencia razona, en su fundamento de Derecho tercero, que «siendo así que la protección que otorga la LORTAD —como ahora sucede con la LOPD— se refiere a los datos de carácter personal de las personas físicas (...) no hay razones para excluir de ese ámbito de protección los datos personales de unos profesionales, en este caso Arquitectos, habida cuenta que, como señala la resolución recurrida, aquellos datos se refieren a profesionales que no ejercen su actividad bajo forma de empresa, no ostentando en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio».

En este mismo sentido, la sentencia niega el razonamiento de que la Ley no es aplicable al tratarse de datos de «agentes económicos que operan en el mercado», dado que la aplicación de dicho razonamiento implicaría que «la protección que nuestro ordenamiento pretende dispensar a los datos de carácter personal quedaría desvirtuada y vaciada de contenido en relación con buena parte de los ciudadanos, conclusión ésta que no resulta conciliable con aquellos postulados que la Ley Orgánica 5/1992 —y ahora la Ley Orgánica 15/1999— sirve de desarrollo.

Por su parte, y frente a la alegación de que la resolución impugnada invertía la carga de la prueba, por cuanto no resulta conforme a derecho que la Agencia impusiera a la recurrente la carga de probar que los datos objeto de tratamiento provenían de fuentes accesibles al público, la Sentencia indica claramente que «aunque a la parte actora le parezca inaudito, lo cierto es que a quien alega haber obtenido los datos de una fuente accesible al público le corresponde acreditar o cuando menos especificar cuál es esa fuente; y debe hacerlo no de manera hipotética o posibilista sino de forma clara y referida a todos y cada uno de los datos cuyo tratamiento y cesión no consentidos se le imputa, pues si la regla general es que tanto el tratamiento como la cesión de datos de carácter personal requieren el previo consentimiento de los afectados y tal exigencia se dispensa sólo en casos de excepción, sólo una especificación del responsable del fichero acerca de la procedencia de los datos permitiría constatar si efectivamente concurre o no el supuesto de excepción alegado».

En consecuencia, dado que el recurrente se había limitado a indicar genéricamente las posibles fuentes de origen de los datos y que por la Agencia se había constatado que los datos no figuraban en dichas fuentes en los términos en que aparecían en el fichero de la propia recurrente, la Sala considera no haber quedado probado que el tratamiento de los datos proceda de fuentes accesibles al público y, en consecuencia, declara ajustada a derecho la sanción impuesta por la Agencia.

Además, la sentencia se refiere a la naturaleza del censo electoral como fuente no accesible al público, siguiendo el criterio ya reiterado y mencionado en anteriores Memorias de esta Agencia, indicando finalmente que la mera indicación administrativa en las obras sitas en la vía pública no puede considerarse como fuente de tal naturaleza, habida cuenta que la misma se efectúa en virtud de una determinada relación contractual o negocial que vincula al profesional con esa obra determinada, aparte por lo demás del hecho de que en dicha indicación no se incluyen todos los datos que se habían incorporado al fichero de la recurrente.

En conexión con la Sentencia analizada, las Sentencias de la Audiencia Nacional de 21 de junio y 11 de octubre de 2002 confirmaron las sanciones impuestas por la Agencia a ciertos Colegios Profesionales que facilitaron a la editorial a la que ha venido haciéndose referencia los datos correspondientes a los proyectos visados por los Colegios en ejercicio de las potestades que la Ley les atribuye, considerando que las corporaciones no habían acreditado la existencia de consentimiento de los afectados ni que la comunicación se refiriese a datos contenidos en fuentes accesibles al público, dado que, como señala la primera de las sentencias citadas, no pueden considerarse como tales los datos relacionados con las personas que intervengan en una construcción por el mero hecho de la existencia de una acción pública en el derecho urbanístico, «porque una cosa es el interés público de que el ius aedificandi se acomode a los dictados de la Ley y al planeamiento urbanístico, y se facilite la posibilidad de que cualquier ciudadano pueda intervenir en pro de la legislación de ese sector, y otra que se pueda traficar libremente con los datos de las personas que intervengan en la actividad económica de la construcción».

3.2.7. Campañas publicitarias. Responsable del fichero y cesiones de datos

La sentencia de la Audiencia Nacional de 21 de junio de 2002 desestima el recurso formulado contra resolución de la Agencia relacionado con la utilización y cesión de datos en el ámbito de una determinada campaña publicitaria.

Dada la complejidad del supuesto, resulta necesario describir los hechos a los que el mismo se refiere con un cierto detalle: La empresa «A», dedicada a la comercialización de deter-

minados productos, contrata con la empresa «B», que presta servicios de publicidad y planificación de campañas, la realización de una determinada campaña, en que partiendo de las indicaciones de «A», «B» queda encargada de obtener los registros correspondientes a los individuos relevantes para la campaña, la impresión de las cartas a enviar, su ensobrado, franqueo y envío a los afectados.

«B» obtiene los datos de una tercera empresa «C», dedicada a la manipulación de correspondencia y envíos diversos. Los datos, a su vez, son comunicados a las empresas «D» y «E», encargadas de la manipulación, impresión de las cartas, ensobrado y envío. Según se alega por «B», los datos se comunican directamente de «C» a «D» y «E», sin que aquélla en ningún momento tenga acceso a dichos datos.

La Agencia impone a «B» una sanción por cesión de los datos a «D», sin haber recabado el consentimiento del interesado para ello.

Dentro de la extensa fundamentación jurídica de la Sentencia, que abunda en conceptos que ya se han reproducido en la presente memoria, tales como la forma escrita en que debe materializarse el contrato que vincula al responsable del fichero con el encargado del tratamiento, la sentencia analizada resulta relevante en dos cuestiones esenciales: por una parte, la consideración de la empresa «B» como responsable del tratamiento; y por otra, la apreciación de que los hechos constituyen una cesión de datos de carácter personal, con independencia de que la empresa «B» haya tenido materialmente en su poder los datos cedidos.

En cuanto a la primera de las cuestiones planteadas, la Sentencia, tras recordar el concepto de responsable del fichero contenido en el artículo 3 d) de la LORTAD, vigente al tiempo de producirse los hechos, así como el establecido en el artículo 2 d) de la Directiva 95/46/CE, recuerda que «la figura del responsable del fichero se conecta pues en la Ley con el poder de decisión sobre la finalidad, contenido y uso del tratamiento, poder de decisión que ha de diferenciarse de la realización material de actividades que integran el tratamiento, ya que será el responsable tanto quien decida y trate como quien, teniendo poder de decisión, encomiende la materialidad del tratamiento a un tercero que actúe bajo la dependencia o instrucciones del primero».

«En el presente supuesto —prosigue la resolución— tal y como pone de manifiesto la APD, ha sido («B») quien ha decidido sobre la finalidad, contenido y uso del tratamiento. Sobre la finalidad por haber alquilado los datos a («C») para organizar la campaña de publicidad ya aludida. Sobre el contenido puesto que tales datos alquilados y usados en la campaña eran los de personas que tuvieran determinadas características. Y sobre el uso puesto que era también la entidad actora la encargada de enviar los registros a los destinatarios finales».

Asimismo, se niega la alegación de «B» de no ser más que un mero intermediario entre «A» y «C», puesto que en los envíos recibidos por los afectados se indicaba que los datos habían sido suministrados por «B», ante quien los afectados podían ejercitar sus derechos.

Por otra parte, como se indicó, la recurrente alegó no haber tenido en su poder en momento alguno los datos supuestamente cedidos, toda vez que los mismos fueron comunicados a «D» directamente por «C», tal y como se desprende de un documento aportado por «B» en el procedimiento seguido por la Agencia.

La sentencia, reincidiendo en la consideración de que «B» era responsable del fichero, al poseer el poder de decisión que se ha descrito anteriormente, considera que la cesión existe en todo caso con independencia del contacto material de «B» sobre los datos, dado que la transmisión se habría realizado bajo ese poder de disposición, actuando «C» por encargo de «B».

Así, indica el Fundamento de Derecho sexto de la sentencia que el documento en que la recurrente pretende fundar su no culpabilidad «lo que evidencia es que («B») no tenía necesidad de tener conocimiento de los datos entregados a («D») pero no es prueba suficiente de que tal actora no haya comunicado o revelado tales ficheros informatizados de datos a una persona distinta del interesado o afectado sin consentimiento de sus titulares, conducta que, como ya se ha manifestado con anterioridad, constituye cesión de datos de carácter ilícito, al no estar respaldada por el consentimiento de los titulares de tales datos».

En consecuencia, la sentencia considera que «B», ya sea directamente, ya sea a través de «C», ha comunicado los datos de carácter personal a «D» sin consentimiento de los afectados, conducta contraria a lo dispuesto en la entonces vigente LORTAD y, en la actualidad, a la LOPD.

3.2.8. Utilización de datos personales de abonados a servicios telefónicos

La Sentencia de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid de 16 de julio de 2002 viene a resolver finalmente el recurso formulado contra resolución de la Agencia, de 6 de junio e 1997 en que se sancionaba a una empresa filial de un determinado operador de telecomunicaciones.

Los hechos son analizados con detalle en la Memoria correspondiente a 1997 (págs. 148 a 152), si bien pueden resumirse del siguiente modo:

La entidad sancionada tiene por objeto social la actividad publicitaria de todo género así como la confección para su matriz de directorios de abonado. A tal fin, la operadora le

remitía mensualmente un fichero de información de sus abonados en el que, junto con la información necesaria para la publicación de los directorios, facilitaba otra información (hasta 44 datos), referida al nivel de facturación, oficina de domiciliación, etc.

La entidad recurrente completaba dicha información con otros datos obtenidos estadísticamente por el cruce con otros ficheros, incluyendo la «sección censal» publicada por el Instituto Nacional de Estadística. Además, otros datos se deducían de los ya obtenidos, tales como el sexo, el hábitat rural o urbano de residencia o el tipo de vivienda a partir del dato del domicilio.

La recurrente empleaba los datos del fichero con la finalidad de alquilarlos a otras entidades para la realización de campañas publicitarias a partir de la segmentación que se alcanzaba de la combinación final de más de 70 datos correspondientes a más de 11 millones de hogares.

La argumentación del recurso se centraba en la consideración de los datos obtenidos como «públicos», lo que eximía de la obtención del consentimiento de los afectados tanto para su recogida y tratamiento como para su cesión ulterior mediante alquiler a otras empresas. Este argumento no es acogido por la Sentencia a la que nos referimos, partiendo en primer lugar de que la mayor parte de los datos suministrados por la operadora de telecomunicaciones, tales como la facturación, los equipos instalados o el sistema de cobro de las facturas, no tenían ningún carácter público.

Así se indica que «no hay duda de que estos datos no son públicos y es imposible adquirirlos cruzando o tratando automatizadamente los que constan en las guías telefónicas con los difundidos por los organismos públicos, por más perfecto que sea el proceso informático empleado. Además, la naturaleza de los datos sólo permite atribuírselos a (el operador), entidad a la que son suministrados por el cliente a efectos de concertar y ejecutar el contrato de servicio telefónico».

A mayor abundamiento, la sentencia considera que algunos de los datos son obtenidos «mediante la aplicación de complejos procedimientos informáticos y a través del uso de informaciones a disposición el público en general».

En este sentido recuerda lo establecido en la Exposición de Motivos de la LORTAD, vigente al tiempo de producirse los hechos, en cuanto a la posibilidad de que una serie de datos aislados pueda arrojar un perfil completo del individuo que, precisamente, es lo que el artículo 18.4 de la Constitución pretende impedir, señalando que tal conducta es exactamente la llevada a cabo por la recurrente, que efectuaba un detallado proceso de segmentación y microsegmentación que permitía la identificación de perfiles sumamente detallados de los individuos y hogares. Así, concluye, «la referida conducta configura una modalidad de tratamiento

de datos mediante su elaboración, con arreglo a la definición del artículo 3 c) de la Ley que, sin consentimiento del afectado, también es objeto de prohibición por el artículo 6.1».

Por último, la sentencia aclara que la invocación de que no se ha producido un daño efectivo como consecuencia de esta conducta no resulta suficiente para excluir la reprensibilidad de la misma, confirmando las sanciones impuestas por la Agencia, tanto por tratamiento como por cesión ilegal de datos de carácter personal sin contar con el consentimiento del afectado.

3.2.9. Sentencia en recurso contra la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos

Especial análisis merece la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 15 de marzo de 2002, que resuelve la impugnación directa de la Instrucción 1/2000 de la Agencia, particularizada, como la propia Sentencia pone de manifiesto en algunas de sus normas (apartado 2 de la Norma Tercera, apartado 1 de la Norma Cuarta, apartados 1 y 2 de la Norma Quinta la Norma Sexta en su totalidad).

El fallo de dicha sentencia señala literalmente «que estimando en parte el recurso contencioso-administrativo interpuesto (...) contra 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, debemos anular y anulamos el apartado 2 de la Norma Tercera y la Norma Sexta de dicha Instrucción, si bien ambos en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la Ley Orgánica 15/1999, y anulamos también el apartado 1 de la Norma Cuarta de la misma Instrucción, desestimando en lo demás la pretensión de la demandante, sin imponer las costas de este proceso a ninguno de los litigantes».

En consecuencia, salvo en lo referido al apartado 1 de la Norma Cuarta, la Sentencia no declara una anulación real de la Instrucción, sino que sólo prohíbe la interpretación de determinadas normas de la misma de forma que ello obstaculice el régimen previsto en el artículo 34: En resumen, no será posible que, en caso de que un responsable del tratamiento pretenda efectuar una transferencia internacional de datos de carácter personal amparada en una de las causas del artículo 34 de la LOPD, la Agencia exija para llevarla a cabo una autorización de su Director, en los términos previstos en el artículo 33.1 de la misma.

Entrando ya en el estudio de la Sentencia, su Fundamento Jurídico tercero describe el régimen establecido en los artículos 33 y 34 de la LOPD, partiendo de la regla de autorización contenida en el primero de ellos, que habrá de complementarse con las excepciones pre-

vistas en el artículo 34. De este modo, concluye la Sentencia, el legislador ha establecido un doble régimen en materia de trasferencias internacionales de datos, diferenciando las sometidas o no sometidas a autorización del Director de la Agencia, según concurra o no una de las causas previstas en el artículo 34; todo ello sin perjuicio del deber de notificación de la transferencia a efectos de su inscripción en el RGPD. Por este motivo, en caso de que la transferencia se funde en una de las causas del artículo 34, no será posible que la Instrucción exija la autorización del Director de la Agencia.

Concluye el citado Fundamento que «la existencia de las mencionadas excepciones a la regla general en modo alguno significa, claro es, que en estos supuestos de inexigibilidad de la autorización previa el responsable del fichero que promueve la transferencia de datos quede liberado del conjunto de deberes y obligaciones que le impone la Ley Orgánica 15/1999; ni que pueda eludir las responsabilidades derivadas de su actuación. Únicamente queda liberado de la exigencia de autorización expresa de la transferencia por el Director de la Agencia, y ello por disponerlo así de manera expresa el artículo 34».

Tomando como referente esta exposición, la sentencia señala en su fundamento quinto que «para determinar si estas disposiciones contenidas en el apartado 2 de la Norma Tercera de la Instrucción son o no ajustadas a derecho resulta imprescindible diferenciar —aunque la Norma examinada no lo hace— según que vengan referidas a las transferencias de datos sujetas a autorización previa o, por el contrario, a cualquiera de los supuestos de excepción enumerados en el artículo 34 de la Ley Orgánica 15/1999», añadiendo que, según la Sala «el problema de partida que presenta este apartado 2 de la Norma Tercera es, precisamente, que pretende referirse de manera indistinta a toda clase de transferencias internacionales de datos, siendo así que, por imperativo legal, el margen de actuación y las posibilidades de intervención de la Agencia son muy distintos en uno y otro caso».

De este modo, si bien no resulta duda alguna de la plena aplicación del precepto al primero de los supuestos planteados, sí cabría, según indica la sentencia, objetar que en el segundo de ellos la potestad de la Agencia no puede llevar nunca a la existencia de un procedimiento encubierto de autorización.

Así se añade que «es precisamente esta vocación expansiva la que nos lleva a concluir que el apartado 2 de la Norma Tercera de la Instrucción no puede ser considerado ajustado a derecho en la medida en que pretende ser aplicable en los supuestos de excepción».

En consecuencia, y tras volver a recalcar en su Fundamento noveno que, tal y como indica el apartado primero de la Norma Segunda de la Instrucción, la transferencia no puede impedir el cumplimiento de la Ley Orgánica 15/1999 ni limitar las potestades que la misma atribuye a la Agencia, «no resulta aceptable que estas potestades de comprobación o incluso de inspección encaminadas asegurar el cumplimiento de la Ley las ejerza la Agencia pre-

cisamente al tener conocimiento de que se pretende realizar una transferencia de datos para la que no es necesaria su autorización».

Por todo ello, la Sentencia declara la nulidad del apartado 1 de la Norma Cuarta y el apartado 2 de la Norma Tercera en cuanto su aplicación contravenga el criterio expuesto.

Por su parte, en el Fundamento décimo se declara la plena validez de la Norma Quinta de la Instrucción. Dentro de su contenido resulta especialmente relevante que la Sentencia señala «en la hipótesis del apartado 1 la Norma se limita a señalar que la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación. Nada hay que objetar a esta previsión, pues, como ya anteriormente tuvimos ocasión de señalar, si el responsable del fichero alega encontrarse en un supuesto de excepción en los que la transferencia de datos no necesita autorización. Resulta procedente que la Agencia pueda solicitar alguna justificación que le permita constatar que efectivamente concurre la circunstancia alegada».

Por último, en cuanto a la Norma Sexta de la Instrucción, el fundamento undécimo efectúa un razonamiento similar al que se ha expuesto en relación con el apartado 2 de la Norma Tercera.

A la vista de lo indicado, del tenor de la sentencia se deduce que, sin perjuicio de la potestad de que «la Agencia pueda solicitar alguna justificación que le permita constatar que efectivamente concurre la circunstancia alegada», dentro de las recogidas en el artículo 34 de la LOPD, lo que no será posible es exigir una específica autorización para dicha transferencia.

Por último, debe indicarse que la sentencia que ha venido analizándose ha sido objeto de recurso de casación ante la Sala Tercera del Tribunal Supremo, por lo que habrá de estarse a la decisión de dicho recurso.

3.3. Sentencias del Tribunal Supremo en materia de protección de datos de carácter personal

Como ya se indicó, durante 2002 se han dictado por el Tribunal Supremo 9 sentencias relacionadas con resoluciones de la Agencia de Protección de Datos, además de dos Autos inadmitiendo sendos recursos contra sentencias que desestimaron los interpuestos contra resoluciones de la Agencia.

De las 11 sentencias, 8 confirmaron el criterio de la Agencia y sólo 3 declararon haber lugar al recurso.

Las sentencias pueden organizarse en cuatro grupos básicos, dado que varias de las mismas guardan similitud en las materias planteadas. Por ello, las analizaremos en atención a esa clasificación.

3.3.1. Invocación de la aplicación del artículo 45.5 de la LOPD

Cuatro de las sentencias indicadas rechazan la pretensión del recurrente de aplicar retroactivamente a la sanción impuesta el artículo 45.5 de la LOPD, según el cual «Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate».

Concretamente, cabe hacer referencia a las Sentencias de 18 de marzo, 12 de abril, 18 de abril y 22 de noviembre de 2002 (todas ellas dictadas en recursos de casación para unificación de doctrina), que contienen pronunciamientos en ese sentido, rechazando en todo caso la aplicación de la norma invocada.

En las sentencias de 18 de marzo y 12 de abril de 2002, la pretensión es desestimada por el hecho de no haberse efectuado por la recurrente en instancia alegación alguna en este sentido, no probándose la existencia de circunstancias que permitiesen analizar su aplicación.

Así, la Sentencia primeramente citada señala que «en el presente caso, la recurrente simplemente alega que distintas sentencias anteriores de la Sala de la Jurisdicción de la Audiencia Nacional hicieron aplicación de un precepto que no se invocó en su demanda por el recurrente ni se aplicó en el caso de la recurrida, lo que por sí solo habría de dar lugar a la desestimación del recurso, puesto que, evidentemente, no concurre el requisito exigible conforme al artículo 96.1 de que el pronunciamiento de la sentencia llegue a resultados diferentes con fundamentos y pretensiones sustancialmente iguales».

Concluye la sentencia que «tampoco existe identidad de pretensiones, puesto que, a diferencia de las razones concurrentes en aquellos otros recursos y que, a diferencia de las razones concurrentes en aquellos otros recursos y que dan lugar a la aplicación de dicho precepto por la Sala, ocurre que en la sentencia recurrida ni se enjuiciaron esas especiales circunstancias determinantes de la aplicación del citado artículo 45 ni, desde luego, se formuló cuestión o pretensión alguna en la demanda del recurso de instancia sobre la aplicación o no al caso del precepto repetidamente transcrito.

En la sentencia de 18 de abril de 2002, la Sala ahonda en este criterio, indicando que «La aplicación de esa norma nueva introducida por la LORTAD de 1999 exige una valoración de las circunstancias concurrentes en el caso y la parte recurrente, ni en la instancia ni en este recurso, hace la menor referencia a este extremo. Simplemente dice que puesto que el precepto existe y la sentencia de contraste lo aplicó debió aplicarse también por la Sala que dictó la sentencia impugnada. Pero esto no es lo que dice el artículo 45.5 de la nueva LORTAD, que hemos transcrito más arriba. Debiéndose notar también porque es un dato más que revela esa falta de identidad sustancial, que en el caso de la sentencia de contraste y al hilo precisamente de los argumentos que proporciona la entidad bancaria recurrente —entre ellos que pudo haberse aplicado el artículo 43.2 c) que tipificaba como infracción leve el no conservar actualizados los datos de carácter personal que consten en los ficheros—, la Sala de instancia pudo obtener el conocimiento de la concurrencia de esas circunstancias».

Al propio tiempo, la sentencia pone de manifiesto una importante doctrina relacionada con los supuestos en que sería admisible la aportación de una sentencia de contraste que pudiera permitir la prosperabilidad del recurso, señalando claramente que la misma debería referirse a una sanción impuesta por la infracción del mismo tipo de la LOPD que la impuesta al recurrente.

Así, el Fundamento de Derecho tercero de la sentencia, después de señalar los términos en que aparecen tipificadas las infracciones contenidas en la sentencia recurrida y la de contraste, indica que «Es claro, sin necesidad de mayor análisis, que aquí falta esa identidad sustancial cuya concurrencia es necesaria para que pueda prosperar un recurso de casación para unificación de doctrina, pues si hay algo verdaderamente decisivo que permite apreciar la existencia o no de identidad sustancial cuando de la aplicación del derecho administrativo sancionador se trata es, precisamente, el tipo de la actuación reprochada por el mismo», añadiendo que «Esto basta, sin más, para concluir que el presente recurso debe ser rechazado totalmente».

Por último, la Sentencia de 22 de noviembre de 2002 acoge los argumentos mantenidos en la jurisprudencia que se ha venido citando.

3.3.2. Utilización de los datos del censo electoral con fines de publicidad y prospección comercial

A lo largo del año 2002 el Tribunal Supremo ha dictado dos sentencias relacionadas con la actividad de empresas dedicadas a la publicidad y prospección comercial, de fechas 26 de abril y 23 de septiembre. De ambas, sólo la segunda se encuentra directamente vinculada con actividades de esta naturaleza, dado que la primera, desestimatoria del recurso interpuesto contra Sentencia del TSJ de Madrid, por la que se desestimaba a su

vez el recurso interpuesto contra resolución sancionadora de la Agencia por la comisión de una infracción de obstrucción a la labor inspectora, se refiere en su fundamentación jurídica a determinados vicios procesales alegados por la recurrente y no a cuestiones de fondo.

Entrando así en el estudio de la Sentencia de 23 de septiembre de 2002, la misma se refiere al supuesto, ampliamente analizado en Memorias correspondientes a años anteriores, en que una empresa dedicada a la actividad de publicidad o prospección recogía y trataba datos de carácter personal provenientes de las listas del censo electoral publicadas a fines de comprobación por los ciudadanos.

En relación con esta materia, la sentencia, que desestima el recurso y confirma la resolución de esta Agencia indica en su Fundamento de Derecho tercero que «La parte recurrente, partiendo de la premisa de que el artículo 39.3 de la Ley de Comercio Minorista contiene una declaración general de accesibilidad al público respecto del nombre, apellidos y domicilio de las personas que figuran en el censo electoral, considera que las empresas dedicadas a publicidad y a la venta directa tienen derecho a obtener determinados datos del censo electoral a fin de desarrollar sus legítimas actividades, ya que los datos de carácter personal provenientes del censo electoral se utilizaron en el momento de la elaboración de aquel, en el que los datos de los electores son expuestos al público y, consiguientemente, son susceptibles de ser conocidos por cualquier persona, pues durante este período los datos electorales son accesibles al público, puesto que se encuentran, según el artículo 1.3 del Real Decreto 1332/1994, «a disposición del público en general» y, por consiguiente, eran aplicables las normas de la Ley Orgánica 5/1992, que autorizan el uso de tales datos sin necesidad de obtener el consentimiento previo de los afectados.

Esta tesis supone una interpretación fragmentaria de dicha disposición, que, en contra del parecer de la representación procesal de la sociedad recurrente, no se limita a formular una declaración de accesibilidad al público del nombre, apellidos y domicilio de electores, sino que, dada su exclusiva finalidad de ordenar el comercio minorista y concretamente las ventas a distancia, se remite expresamente el régimen establecido al efecto por la Ley Orgánica 5/1992, de 29 de octubre, Reguladora del Tratamiento Automatizado de los Datos de Carácter Personal, que, a su vez, contiene en su artículo 2.3.a) una remisión a la legislación de régimen electoral en cuanto al censo electoral y, además, excluye del régimen general de su artículo 11.2.b) —cesión sin consentimiento del afectado de datos recogidos de fuentes accesibles al público— los ficheros de titularidad pública —artículo 19.3—, para cuya cesión o transferencia de datos a ficheros de titularidad privada se requiere el consentimiento del interesado».

Asimismo, la Sentencia desestima las pretensiones del recurrente tomando en consideración la regulación contenida en la ahora vigente LOPD, al señalar, en su Fundamento

cuarto, que «La exégesis que acabamos de hacer se corrobora por el método contemplado en la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, para la confección del denominado «censo promocional» (artículo 31) con el nombre, apellidos y domicilio que consten en el censo electoral, pues se prevé que en el documento de empadronamiento el interesado pueda solicitar no aparecer en el indicado censo promocional, de manera que si al cumplimentar dicho documento de empadronamiento, que constituye la base para la formación del censo electoral, el ciudadano manifiesta su oposición a aparecer en el censo promocional, su nombre, apellidos y domicilio, aunque figuren en el censo electoral, no podrán incluirse en el «censo promocional», único del que pueden servirse para sus lícitas actividades las empresas dedicadas a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras análogas, con la particularidad añadida de que el plazo de vigencia del censo promocional es de un año, transcurrido el cual la lista pierde su carácter de fuente de acceso público, debiéndose editar, además, trimestralmente una lista actualizada del censo promocional con exclusión de los nombres y domicilio de quienes así lo soliciten».

3.3.3. Tratamiento de datos de clientes en casinos de juego

La Sentencia del Tribunal Supremo de 1 de julio de 2002 desestima el recurso de casación interpuesto contra sentencia del TSJ de Madrid de 2 de abril de 1998, que a su vez confirmó una resolución de la Agencia por la que se sancionaba a un determinado casino de juego por tratamiento de datos sin consentimiento del afectado.

El citado casino recogía los datos referidos al gasto efectuado por sus clientes, así como la indicación de sus pérdidas y ganancias sin haber solicitado el consentimiento de los mismos y sin haber siquiera notificado este tratamiento al RGPD para su inscripción. Por parte de la recurrente se alegaba que el tratamiento era necesario para el mantenimiento de las relaciones contractuales con sus clientes, encontrándose así amparado en el artículo 6.2 de la LORTAD, vigente al tiempo de producirse los hechos.

La Sentencia niega que el supuesto tenga encaje en la excepción prevista, respecto al consentimiento del afectado, en el número 2 del artículo 6 de la LORTAD «pues, aun cuando se admitiera que el afectado estaba vinculado por una relación negocial con el Casino, es lo cierto que dichos datos no eran necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato ya que, según expresa la sentencia que se recurre, en función del listado obrante en el expediente en el mismo, contrariamente a lo que se defiende en este recurso de casación, no se recogían exclusivamente los pagos efectuados por cheque sino también los efectuados en metálico y con billetes en mesa, sin que conste dato alguno relativo al buen fin o no de los citados cheques, por lo que no está acreditado que los

datos fueren necesarios para el mantenimiento de las relaciones, al no recogerse exclusivamente los pagos mediante cheques ni constar el control de éstos con independencia de su importe, de donde se deduce la inexistencia de la supuesta infracción del artículo 6 de la Ley Orgánica 5/1992».

Además, la sentencia pone de manifiesto el hecho de que, con posterioridad, el propio casino de juego reemplazó el tratamiento automatizado de datos por un tratamiento manual, «de donde resulta la falta de necesidad de la automatización de los datos obtenidos sin consentimiento del afectado y, en consecuencia, la inexistencia de las infracciones imputadas a la sentencia recurrida que correctamente apreció infracción de lo dispuesto en los artículos 5 y 6 de la Ley Orgánica 5/1992 y, por ello, confirmó la sanción acordada al amparo de lo dispuesto en el artículo 43.3 d) de la Ley Orgánica de 29 de octubre 1992 por tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley»

3.3.4. Responsabilidad por la inclusión de un dato inexacto en ficheros referidos al cumplimiento o incumplimiento de obligaciones dinerarias

Por último, es necesario hacer referencia a la doctrina sentada por la Sentencia del tribunal Supremo de 13 de abril de 2002, reproducida de forma prácticamente literal por las de 29 de julio y 3 de diciembre del mismo año.

Dichas sentencias vienen a resolver sendos recursos de casación para la unificación de doctrina relacionadas con la cuestión, detalladamente analizada en anteriores Memorias de a quién corresponde la responsabilidad por la inclusión de datos incorrectos o inexactos en los ficheros relacionados con el pago o impago de obligaciones dinerarias. A lo largo de una consolidada doctrina, formada por más de 25 sentencias, las salas del TSJ de Madrid y de la Audiencia Nacional habían sentado el criterio de que la entidad informante en estos ficheros era la responsable de la integridad y exactitud del asiento, de modo que a la misma debían dirigirse las actuaciones en caso de detectarse la existencia de infracción de los principios de calidad de los datos. No obstante existieron, esencialmente entre las primeras sentencias dictadas, algunos fallos discrepantes con esta doctrina.

Pues bien, la citada Sentencia de 13 de abril de 2002 viene a resolver por el momento la cuestión, considerando la inexistencia de responsabilidad en el informante, al no ostentar el mismo la condición de responsable del fichero o encargado del tratamiento, por lo que la imposición de la sanción supondría una aplicación analógica de las normas sancionadoras de la protección de datos de carácter personal, proscrita por el artículo 25 de la Constitución.

Esta conclusión se alcanza en el Fundamento de Derecho tercero de la citada sentencia, quizá excesivamente breve en su exposición y razonamiento, que pasamos a reproducir íntegramente:

> «La sentencia recurrida, al extender el régimen sancionador contemplado en la Ley a quien suministró en virtud de un contrato el dato de carácter personal al responsable del fichero, ha conculcado el principio de legalidad consagrado en el artículo25.1 de la Constitución, el artículo 129.4 de la Ley 30/1992, que impide la aplicación analógica de las normas definidoras de infracciones y sanciones, y el artículo 42.1 de la Ley Orgánica 5/1992, de 29 de octubre, en relación con el artículo 3 d) de esta misma Ley, que limita el régimen sancionador al responsable del fichero, cuyo concepto define este último precepto.
>
> En contra del parecer del Abogado del Estado, el responsable del fichero es quien decide sobre la finalidad, contenido y uso del tratamiento automatizado y no quien le facilita el dato en virtud de un contrato celebrado con aquél, de modo que sólo el responsable del fichero está sujeto al régimen sancionador establecido en la aludida Ley Orgánica, que no cabe extender a cualquier otra persona, pues, de hacerlo, como la sentencia recurrida, se incurre en una aplicación extensiva o analógica del régimen sancionador, prohibida por el artículo 25.1 de la Constitución y 129.4 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, con manifiesta conculcación de los principios de legalidad y tipicidad, y por consiguiente la mencionada sentencia debe ser anulada.
>
> La limitación subjetiva del régimen sancionador ha sido mantenida, teniendo en cuenta la lógica del propio sistema, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, al señalar en su artículo 43.1 que «los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley», continuando, por consiguiente, excluidos quienes hubiesen contratado el suministro de datos con aquéllos».

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/CE

La Directiva Europea de Protección de Datos 95/46/CE, 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 (GT29, en lo sucesivo). Es un órgano consultivo independiente en materia de protección de datos y privacidad, dentro de la Unión Europea. Sus funciones se establecen en el Artículo 30 de la Directiva y en el artículo 14 de otra norma comunitaria, la Directiva 97/66/CE, sobre telecomunicaciones.

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 comunitarios así como por un representante de la Comisión.

A las reuniones del GT29 pueden acudir, como observadores, representantes de las Autoridades de Control de los países que forman parte del Espacio Económico Europeo —Noruega, Islandia y Liechtenstein— y 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 GT29 se reunió por primera vez en febrero de 1997 y ha mantenido un total de 36 reuniones —la última tuvo lugar el 25 de noviembre de 2002—, habiendo aprobado hasta dicha fecha un total de sesenta y siete 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 GT29 así como en los encuentros y foros preparatorios de las mismas. En 2002, la Agencia de Protec-

ción 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 del empleo; de la privacidad en Internet y de cláusulas contractuales estándares para la transferencia de datos personales a países que no gozan de un nivel de protección adecuado con el fin de garantizar los derechos de los ciudadanos. El número de reuniones de estos subgrupos fue de doce.

Podemos observar que si bien las sesiones plenarias del GT29 fueron las mismas que el pasado año 2001, sin embargo las de los subgrupos se han duplicado. Esto se debe fundamentalmente a la complejidad técnica de los temas de fondo sobre los que incide el derecho a la protección de datos personales (descripciones técnicas de los nuevos protocolos de Internet, sistemas de identificación *on-line*, etc.) que exige la discusión previa por cualificados expertos sectoriales en cada materia antes de elevarse para su aprobación por el pleno.

El Artículo 30 de 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, 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 un 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 uso de estas funciones, durante el año 2002 el GT29 ha aprobado 14 documentos que se relacionan a continuación[1]:

[1] Los documentos antes relacionados pueden consultarse, en versión española, en la página web del propio GT29, que se indica a continuación, todos ellos se identifican por un número y van precedidos de las siglas WP, correspondientes a Working Party, en inglés:
http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_en.htm).

- Documento de Trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara. Adoptado el 25 de noviembre de 2002.

- Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos. Aprobado el 24 de octubre de 2002.

- Documento de Trabajo sobre las listas negras. Adoptado el 3 de octubre de 2002.

- Dictamen 5/2002, sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones. Aprobado el 11 de octubre de 2002.

- Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina. Adoptado el 3 de octubre de 2002.

- Documento de Trabajo sobre el funcionamiento del Acuerdo de Puerto Seguro. Adoptado al 2 de julio de 2002.

- Dictamen 3/2002 relativo a las disposiciones sobre protección de datos de la propuesta de Directiva relativa a la armonización de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de crédito a los consumidores. Adoptado el 2 de julio de 2002.

- Documento de Trabajo Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea. Aprobado el 2 de julio de 2002.

- Dictamen 2/2002 sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones: ejemplo del IPv6, adoptado el 30 de mayo de 2002.

- Dictamen 1/2002 relativo al Informe del CEN/ISSS sobre la normalización de la protección de la vida privada en Europa. Adoptado el 30 de mayo de 2002.

- Documento de Trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios *web* establecidos fuera de la UE. Aprobado el 30 de mayo de 2002.

- Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Aprobado el 29 de mayo de 2002.

- Quinto Informe Anual sobre la situación sobre la protección de los individuos en cuanto al tratamiento de sus datos personales y su privacidad, dentro de la Unión europea y en Terceros Países, durante el año 2000. Aprobado el 6 de marzo de 2002.

De todos los Dictámenes y Documentos de Trabajo adoptados por el GT29 durante el 2002, vamos a centrarnos a continuación en aquellos asuntos que han sido especialmente relevantes y que por su importancia requieren una mayor atención en esta Memoria, habiendo participado de forma muy directa en todos ellos la Agencia de Protección de Datos.

1.1. La protección de datos personales y las medidas internacionales de lucha contra el terrorismo

Dos son los documentos aprobados durante el año 2002 por el GT29 que tienen su fundamento último en medidas adoptadas para luchar internacionalmente contra el terrorismo: el Dictamen 5/2002, sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones, que se reproduce íntegramente en el apartado dedicado a dicha Conferencia en esta Memoria y el Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos (ver WP 64 y WP 66).

En ambos casos, la Agencia de Protección de Datos manifestó, conjuntamente con sus colegas europeos, cuál es la opinión y los criterios que deben presidir la transmisión de datos personales en los supuestos planteados, para respetar la normativa comunitaria y nacional vigente.

En relación con el Dictamen 6/2002 y dada la enorme trascendencia que para la protección de datos en el ámbito del transporte internacional de pasajeros va a tener este asunto, vamos a explicar como se generó y cuál es su contenido.

A raíz de los atentados del 11 de septiembre de 2001, los Estados Unidos aprobaron, el 19 de noviembre de 2001, la *Aviation and Transportation Security Act* (Ley sobre seguridad en el transporte y la aviación), que exige que las compañías aéreas que operen en su territorio les faciliten los datos relativos a los pasajeros y la tripulación (*Passenger Manifest Information*). Estas transferencias se realizarán en un medio electrónico y deben ser completadas, como máximo, quince minutos después del despegue del avión. A pesar de que el «*Commissioner of Customs*» (Comisario de Aduanas) es el receptor de los datos enviados a los Estados Unidos, las autoridades federales de dicho país también dispondrán de estos datos. El propósito de la transmisión de datos no solo atañe a la seguridad de la aviación, sino que constituye un asunto de orden público en los Estados Unidos.

El 14 de mayo de 2002, los Estados Unidos aprobaron otra ley para reforzar la seguridad fronteriza, que exige que las compañías aéreas cuyos vuelos entren o salgan de este país transmitan los datos relativos a los pasajeros y la tripulación al *US Immigration and Naturalization Service* (Servicio de Inmigración y Naturalización de los EE.UU.). En lo que respecta a los pasajeros y la tripulación que salgan de los EE.UU., las transferencias se han de realizar en un medio electrónico, y deben completarse 15 minutos antes del despegue del avión, para que sea posible actualizar o corregir la lista de pasajeros en un espacio máximo de 15 minutos después de la salida. El *US Immigration and Naturalization Service* se reserva el derecho de exigir, si lo considera necesario, que el vuelo regrese al aeropuerto de los EE.UU. en el plazo de una hora desde su salida. Todos los datos deben transmitirse a una base de datos centralizada conjunta del *US Customs* (Servicio de Aduanas de los EE.UU.) y el *Immigration and Naturalization Service*. Una vez hayan sido transmitidos, estos datos se compartirán con otras agencias federales.

A lo largo del tiempo, APIS[2] ha experimentado numerosos avances significativos, especialmente la ampliación de su lista de datos. Al principio, los datos requeridos estaban intrínsecamente relacionados con el vuelo tomado, el visado o el permiso de residencia para los Estados Unidos, así como con información identificativa como la que figura en los pasaportes. En particular, la reciente ley estadounidense sobre seguridad fronteriza exige que, para los vuelos que entren y salgan de los EE.UU., se transmitan los siguientes datos a la Oficina de Inmigración de este país: nombre, fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los EE.UU., lugar y fecha de expedición (si corresponde), número de registro extranjero (si corresponde), domicilio en los Estados Unidos durante la estancia, así como cualquier otro dato que se considere necesario para identificar a los viajeros, aplicar las normativas sobre inmigración y proteger la seguridad nacional.

Además, en la actualidad (Norma provisional. Registro Federal, 25 de junio de 2002), información sobre el registro de pasajeros (*Passenger Name Record Information*) obligatoria para los pasajeros de vuelos de matrícula extranjera que entren o salgan de los Estados Unidos se exige, previa petición, la transferencia de datos tratados mediante las reservas y los sistemas de control de salidas (DCS), en especial el llamado *Passenger Name Record* (PNR,

---

[2] APIS: Advanced Passenger Information System. Información que con carácter previo a la llegada de un vuelo debe suministrarse a las autoridades americanas respecto de cada pasajero y miembro de la tripulación. En un primer momento se refería únicamente al vuelo en el que se viajaba, el visado e información identificativa como la que figura en los pasaportes. Posteriormente, se vio ampliada con información referente a fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los EE.UU., lugar y fecha de expedición (si corresponde), número de registro extranjero (si corresponde), domicilio en los Estados Unidos durante la estancia, así como cualquier otro dato que se considere necesario para identificar a los viajeros, aplicar las normativas sobre inmigración y proteger la seguridad nacional.

registro de nombres de los pasajeros[3]). Los datos en cuestión no se refieren únicamente a los pasajeros que vuelen a los Estados Unidos, y pueden variar según las distintas compañías aéreas. Pueden referirse a datos identificativos (apellidos, nombre, fecha de nacimiento, número de teléfono), número de reserva del PNR, fecha de la reserva, la agencia de viajes cuando corresponda, la información que se muestra en el billete, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de asiento y datos anteriores del PNR. En estos últimos pueden constar no sólo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etc.), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (*Frequent Fliers number*).

Para garantizar la remisión de los datos solicitados, en la normativa mencionada se contempla la aplicación de fuertes sanciones, especialmente la pérdida de derechos de aterrizaje y el pago de cuantiosas multas si no se facilita información, o ésta es incorrecta o incompleta.

En este punto, hay una cuestión que hay que mencionar y es que estas demandas no se realizaron de manera simultánea a todas las aerolíneas europeas sino que la misma afectó, en una misma fase, a un grupo de ellas entra las que figuraba Iberia.

Varias autoridades de control, entre las que se encontraba la APD, solicitaron que el GT29 debatiera este problema y se pronunciase claramente sobre el mismo. El Dictamen del Grupo señaló que si bien es cierto que los Estados soberanos poseen un criterio definido respecto a la información que pueden pedir a las personas que desean acceder a su territorio, no es menos cierto que las propuestas actuales en lo que respecta al sistema APIS y PNR, que se han elaborado en el contexto de execrables crímenes terroristas, podrían llevar a la divulgación desproporcionada y periódica de información por parte de las compañías aéreas que deben atenerse a los requisitos de la Directiva 95/46/CE.

Esta información podría utilizarse con fines regulares relacionados con la inmigración y el control aduanero así como, de un modo más general, para la seguridad nacional de los EE.UU., y podría, al menos, ser compartida por todas las agencias federales de dicho país.

---

[3] El PNR es el registro en el que cada línea aérea almacena toda la información relativa a los datos de reserva de vuelos de los pasajeros.

A la luz del reciente desarrollo de estos sistemas de acceso anticipado a la información sobre los pasajeros, especialmente la relativa al PNR, el GT29 opina que cumplir con las exigencias de los EE.UU. crearía problemas respecto a la Directiva 95/46/CE. La mayoría de las cuestiones en juego se encuentran fuera de la competencia de las compañías aéreas y deberían ser los Estados miembros, y la Comisión, si resultara necesario, quienes se ocupasen de ellas.

En esencia, el GT29 opina que deberían impedirse las transferencias de datos relativos a personas que no viajen a los Estados Unidos, excepto bajo acuerdos específicos de cooperación relacionados con Justicia e Interior. Tan solo serían posibles otros tipos de transmisión de datos desde los sistemas de reserva y de control de salida relativos a los pasajeros y a la tripulación si cumplen con la legislación de los Estados miembros.

Esta legislación nacional debe sujetarse al principio de que toda restricción necesaria de los derechos y obligaciones que figuran en la Directiva 95/46/CE lo haga respetando los términos de su artículo 13 y garantizar el amparo de las personas. Asimismo, se recomienda la conveniencia de que cualquier solución se ponga en práctica desde la perspectiva de la UE.

Las transferencias de los datos que puedan ser considerados especialmente protegidos deberían realizarse con extrema precaución. Del mismo modo, al efectuar estas transferencias se presupone que se pueden ofrecer pruebas de que, en primer lugar, existen motivos de alto interés público para Estados Unidos, en segundo lugar las garantías adecuadas y, por último, que se cumpla la legislación nacional, que puede implicar la necesidad de una decisión o autorización de la autoridad supervisora.

Si además se pone en práctica el acceso directo a los datos de los sistemas de reserva y de control de salida por parte del Servicio de Aduanas y el Servicio de Inmigración y Naturalización de los EE.UU., estas autoridades se deben comprometer a garantizar el respeto a la Directiva en su totalidad. Debería adoptarse una perspectiva global para tratar la transferencia de datos personales por parte de las compañías aéreas a los Estados Unidos. En primer lugar, sería necesario tener en cuenta otras transferencias, existentes o planeadas, a dicho país y sería especialmente necesario incorporar el concepto de Tercer Pilar (cooperación Judicial y Policial).

Esencialmente, las transferencias de datos a las autoridades públicas de terceros países por razones de orden público en este país deberían ser entendidas en el contexto de los mecanismos de cooperación establecidos por medio del Tercer Pilar. Asimismo, estos mecanismos deberían estar estrechamente relacionados con las garantías de protección de los datos transferidos. Parece importante para el buen funcionamiento de los mecanismos de cooperación basados en el Tercer Pilar que no se esquiven pasando, en su lugar, por el Primer Pilar. Por último, la solución a la que se llegue para las transferencias de datos a los Estados Unidos podría resultar apropiada para servir de modelo a las transferencias que se realizan a instancia de otros países distintos utilizando mecanismos similares a los descritos.

El sistema debería negociarse con las autoridades estadounidenses. En particular, los debates deberían centrarse en: aclarar y definir los objetivos, las finalidades y los receptores de los datos; las categorías de los datos que puedan transferirse, habida cuenta de estas explicaciones, y las condiciones y garantías que rodean al tratamiento de datos personales, en particular su envío a las autoridades federales de los EE.UU. (y, si éste se produce, limitarlo a autoridades de las fuerzas de seguridad).

Esta es pues, basándose en la Directiva 95/46/CE, la opinión unánimemente manifestada por todas las autoridades de protección de datos de la Unión Europea en relación con este problema y todas estas consideraciones deberán tenerse muy presentes en las futuras negociaciones que se inicien con las autoridades norteamericanas para alcanzar una solución jurídicamente aceptable.

1.2. El uso de Internet y la protección de datos personales: los sistemas de autenticación on-line

Hay que destacar así mismo la activa participación desarrollada por parte de la APD en el Subgrupo de Trabajo de Internet cuya creación se acordó en el seno del Plenario del GT29 con la finalidad de analizar la problemática y los riesgos para la protección de datos que pueden darse en las redes globales y, en concreto, en Internet. La APD forma parte de otro Subgrupo y ha participado y participa muy directamente en todos sus trabajos. Durante el año 2002, este Subgrupo preparó dos documentos relativos a los servicios de autenticación en línea y al examen de cuál es la protección que se está dando al tratamiento de los datos personales en Internet por sitios *web* establecidos fuera de la UE. Ambas labores se concluyeron de manera fructífera mediante tres importantes documentos de trabajo (WP 56 y 60, en el año 2002 y el WP 68, aprobado en enero de 2003, pero que por su íntima conexión con los trabajos realizados en 2002 y su actualidad, se ha preferido analizar en esta Memoria para no dilatar la difusión de sus resultados en un año).

La finalidad de los servicios de autenticación *on-line* es evitar que los usuarios deban identificarse y autenticarse repetidamente utilizando procedimientos distintos y memorizando contraseñas diferentes. Estos servicios permiten a los usuarios que tienen registrada y verificada alguna forma de identificación (que incluye en ocasiones una dirección de correo electrónico) delegar parte del proceso de autenticación en el proveedor del servicio, que es quien, a petición del usuario, autentica su identidad en todos los sitios participantes.

Los documentos afectan a dos importantes iniciativas actuales: la del sistema de Microsoft *.Net Passport* y la del Proyecto *Liberty Alliance.* Concluye con unas directrices concretas para ser aplicadas por esos servicios y por cualesquiera otros sistemas de autenticación presentes o futuros.

A raíz de las preocupaciones manifestadas por el GT29 en relación con algunos aspectos de *.Net Passport*, Microsoft propuso entablar un diálogo franco y abierto con dicho Grupo, fruto del cual fue un compromiso público de llevar a cabo toda una serie de modificaciones al sistema dentro de unos plazos establecidos para alinearlo con los principios de la Directiva 95/46/CE. En el documento, pues, se expresa también el compromiso asumido por Microsoft de modificar sustancialmente su sistema *.Net Passport*, afectando en particular a un cambio radical en los flujos de información. La consecuencia más importante es que los usuarios se verán informados leal y verdaderamente y tendrán la capacidad de decidir qué datos proporcionan y en qué condiciones esos datos serán procesados por Microsoft o por los sitios *web* participantes.

Los cambios apuntados en el sistema *.Net Passport*, una vez que estén completamente desarrollados, proporcionarán a los usuarios una mejor protección de sus datos personales. El GT29 va a seguir muy de cerca la ejecución y desarrollo efectivo de las medidas anunciadas por Microsoft.

El Documento tiene también un capítulo dedicado al *Liberty Alliance*. Éste es un proyecto *ad hoc* en el que participan diferentes compañías para establecer una serie de niveles de identificación, sin que exista un único proveedor centralizado sino más bien una red de confianza entre los sitios participantes y que utiliza especificaciones técnicas abiertas. Este proyecto se basa en un sistema diferente que no implica la existencia de una base de datos centralizada. El Informe hace unas observaciones a los aspectos que se están manejando en esta primera fase de desarrollo del proyecto y a los aspectos futuros, y directrices de aplicación general para cualquier sistema presente o futuro de autenticación *on-line* y que pueden resumirse de la siguiente manera:

- Todos los actores implicados en los sistemas de autenticación *on-line*, tanto quienes los diseñan y programan como quienes los implementan como sus sistemas de autenticación en línea (proveedores de autenticación) son responsables de la protección de los datos, aunque a niveles diferentes, incluidos los proveedores de servicios que utilizan dichos sistemas.

- Deberá ponerse todo el empeño posible en que puedan utilizarse de manera anónima o seudónima sistemas de autenticación en línea o, en el caso de que esto impida que sean plenamente funcionales, deberán crearse sistemas que exijan una información mínima.

- Es fundamental ofrecer a los usuarios información adecuada sobre las implicaciones para la protección de sus datos personales derivadas de la utilización del sistema (identidad del responsable del tratamiento, fines, datos recogidos, destinatarios, etc.). Deberá facilitarse esta información permitiendo un fácil acceso y utilización, preferiblemente en forma de recopilación o mediante un cuadro indicador que se abra automáticamente en la pantalla del usuario, en todos los idiomas en los que se ofrezca el servicio.

- Cuando los datos personales deban transferirse a terceros países, los proveedores de autenticación deberán trabajar con los proveedores de servicios, que tomarán todas las medidas necesarias para prestar la protección adecuada, sin perjuicio de recordar que los tratamientos realizados por responsables establecidos en la UE deben someterse a los términos de la Directiva 95/46/CE. Si en casos concretos se emplea el consentimiento como base de la transferencia, deberá proporcionarse a los usuarios suficiente información y posibilidad de elección.

- La utilización de identificadores únicos, en cualquiera de sus formas, acarrea riesgos para la protección de los datos. Deberán estudiarse a fondo todas las alternativas posibles.

- Se valoraría la adopción de una arquitectura de software que reduzca al mínimo la centralización de los datos personales de los usuarios de Internet.

- Los usuarios deberán contar con un medio sencillo para ejercer sus derechos, incluidos los de oposición y cancelación. También deberían recibir información adecuada sobre el procedimiento que han de seguir si desean formular preguntas o reclamaciones.

- La seguridad desempeña un papel fundamental en este ámbito, por lo que deben tomarse las medidas organizativas y técnicas adecuadas a los riesgos que se corren.

Asimismo, el GT29 toma nota de las preocupaciones manifestadas por Organizaciones no Gubernamentales y anima a aquellos que diseñan o desarrollan sistemas de autenticación *on-line* a tomar en consideración estas directrices que se contienen en el Documento para asegurar que los sistemas respeten los requisitos de la Directiva.

Debido a la naturaleza evolutiva del sistema *.Net Passport*, del proyecto *Liberty Alliance* y de otros sistemas similares de autenticación *on-line*, el GT29 continuará vigilando los futuros desarrollos en este campo. En especial, hay dos cuestiones que requieren una mayor atención: las actuales comunicaciones comerciales electrónicas dentro de *Hotmail* y el uso de los identificadores tanto del sistema *.Net Passport* como del proyecto *Liberty Alliance*.

Durante los próximos meses el Subgrupo Internet realizará un seguimiento de los compromisos adquiridos por Microsoft.

Asimismo, dentro del amplio espectro de problemas que puede plantear el uso de Internet para la protección de datos personales y la defensa de la privacidad, el GT29 se ha ocupado de asunto tan difícil como controvertido, la legislación aplicable al tratamiento de datos personales que se hace en Internet por sitios *web* establecidos fuera de la UE. A tal efecto aprobó el 30 de mayo un documento en cuya redacción participó decisivamente esta Agencia (ver WP56).

En él se parte de las consideraciones incluidas en otro documento previo denominado «Privacidad en Internet» del año 2000, donde se señalaba la necesidad evidente de remitirse a la norma relativa a la legislación aplicable de la Directiva de Protección de Datos (Artículo 4.1 letra c), en particular para el tratamiento *on-line* de datos personales por un responsable establecido fuera del territorio comunitario.

La necesidad de determinar si el Derecho nacional se aplica a las situaciones en las que intervienen varios países no es específica de la protección de datos, ni de Internet, ni de la Unión Europea. Se trata de una cuestión general de Derecho internacional que se plantea en situaciones *on-line* y no *on-line*, cuando intervienen uno o más elementos que afectan a más de un país. Es necesario decidir sobre la legislación aplicable para poder desarrollar una solución sobre el fondo.

En el Documento se hace un interesante estudio del artículo 4 de la Directiva de Protección de Datos, uno de los más polémicos de esta norma Comunitaria. Este artículo plantea la cuestión de la legislación aplicable a operaciones de tratamiento de datos personales en los casos en los que al menos un aspecto del tratamiento sobrepasa las fronteras del Estado miembro.

Se analizan también en el propio Documento cuáles son los factores pertinentes para determinar la legislación aplicable: el establecimiento, el responsable del tratamiento y los medios empleados para el mismo.

Tras examinar algunos ejemplos prácticos como son los *cookies*, *JavaScript*[4], *banners* y otras aplicaciones similares, el GT29 concluye que sólo podrá garantizarse un nivel elevado de protección de los particulares si los sitios *web* establecidos fuera de la Unión pero que utilizan medios situados en el territorio comunitario respetan las garantías para el tratamiento de los datos personales, en particular la recogida, y los derechos personales reconocidos a nivel europeo y aplicables de todas formas a todos los sitios *web* establecidos en la Unión Europea.

---

[4] Los JavaScripts son aplicaciones informáticas enviadas por un sitio web al ordenador de un usuario que permiten a servidores remotos ejecutar aplicaciones en el PC del usuario. En función del contenido del programa informático, los JavaScripts permiten mostrar información en una página web, pero también introducir virus en el ordenador (los denominados Java malignos) o recoger y tratar información personal almacenada en el ordenador.

Además, considera que el desarrollo de un programa de promoción de normas europeas pragmáticas de protección de datos ayudaría también a los responsables del tratamiento de terceros países a comprender, aplicar y demostrar mejor el respeto de la privacidad. Un sistema europeo de etiquetas/sellos *web* , abierto también a sitios *web* no europeos, podría ser la base de esta iniciativa.

1.3. La protección de datos personales y la seguridad de los ciudadanos: la videovigilancia

El 25 de noviembre de 2002 el GT29 aprobó someter a consulta pública un Documento sobre videovigilancia (consultar WP 67, en la dirección inicialmente descrita). Con él se pretende contribuir a la aplicación uniforme, en los distintos Estados miembros, de las medidas que prevé la Directiva 95/46/CE en éste área.

Se considera fundamental que los Estados Miembros proporcionen directrices e instrucciones a los productores, proveedores de servicios, distribuidores, investigadores y cualesquiera otros sujetos que desarrollen tecnologías y software de videovigilancia, a fin de que lo hagan de acuerdo con los principios que se recogen en el documento.

El Documento hace un estudio de las legislaciones comparadas dentro de la UE que regulan la videovigilancia y analiza a continuación los casos en que los principios de la Directiva 95/46/CE deben aplicarse y aquellos que quedan fuera de su ámbito: seguridad nacional, defensa e investigación criminal.

Los puntos más importantes de este Documento son aquellos en los que se define cuándo la captación de imágenes y sonidos de una persona deben considerarse datos personales; cuándo hay tratamiento de datos personales mediante videovigilancia; y qué obligaciones y precauciones deben asumir los responsables de dicho tratamiento.

Éstas obligaciones coinciden con los principios recogidos en los artículos 6 y 7 de la Directiva 95/46/CE, donde se explican los criterios que debe reunir todo tratamiento de datos para ser legítimo (legitimidad y especificidad del fin para el que se captan y recogen dichos datos; consentimiento del sujeto; adecuación y proporcionalidad de los medios empleados con los fines que se pretenden alcanzar; retención de datos por un periodo de tiempo corto y adecuado a las necesidades del tratamiento; información a los sujetos de la existencia de cámaras de videovigilancia, etc.).

Merece especial atención también, la videovigilancia en el marco de las relaciones laborales donde se admite su uso sólo dentro de las facultades de control de la productividad del empresario o para garantizar la seguridad y la salud laboral, siempre con las debidas salvaguardas y garantías y nunca en los lugares de uso privado de los trabajadores, tales como aseos, vestuarios, etc.

El Documento está sometido a consulta pública en todos los Estados Miembros. La página *web* de la Agencia española de Protección de Datos informa a los ciudadanos de tal consulta y facilita el enlace con la página correspondiente de la Comisión europea.

1.4. La protección de datos personales y las denominadas «listas negras»

La iniciativa de este Documento adoptado por el GT29 en octubre de 2002 (ver WP 65, en la dirección inicialmente descrita) corresponde a la Agencia, y responde a una inquietud extendida en la sociedad española sobre las interferencias en la esfera individual de las personas (en su buen nombre y su reputación) que se generan por la incorporación de las mismas a bases de datos en las que se aparece identificado en relación con una situación o hechos determinados.

Nos estamos refiriendo al fenómeno actualmente denominado como «listas negras», cada vez más extendido y de difícil definición por varias razones, ya que independientemente de la dificultad de determinar de manera uniforme su concepto y naturaleza, deben tenerse en cuenta las diferentes regulaciones en los Estados miembros, motivadas por las distintas tradiciones legales y constitucionales de cada uno de ellos.

Si intentamos hacer una aproximación al concepto básico de lista negra, podríamos definirlo como la recogida y difusión de información relativa a un grupo de personas, elaborada de conformidad con determinados criterios (dependiendo del tipo de lista negra en cuestión), que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma.

Estos efectos adversos pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación. Nos referimos por ejemplo a los ficheros de deudores y servicios de información de solvencia patrimonial y crédito; a las listas negras de infracciones criminales; a las listas negras sobre detección de fraude; y a otras, entre las que podríamos citar los ficheros con datos adversos sobre trabajadores o candidatos a un puesto de trabajo, ficheros relacionados con cuestiones de salud, comportamientos sociales o políticos y negligencias de profesionales en el ejercicio de su actividad.

Tras el análisis realizado en el documento, se extraen dos conclusiones fundamentales: de una parte, los claros efectos perjudiciales de esta tipología de ficheros en la esfera privada y social de los individuos, y de otra, la existencia de profundas diferencias en la regulación de la tipología de ficheros en cada uno de los Estados miembros.

De ahí la importancia de destacar, en términos generales, la conveniencia de disponer de criterios uniformes y armonizados que arbitren fórmulas que garanticen a los afectados el ejercicio de los derechos reconocidos en la normativa que protege el derecho a la intimidad y a la protección de datos personales.

Las conclusiones del GT29 recomiendan que sería precisa una armonización en los aspectos siguientes:

- Determinar de forma clara y transparente la tipología de datos personales susceptibles de ser tratados, la finalidad de su tratamiento y las garantías a disposición de los afectados (es decir, establecimiento de sistemas de verificación e instrumentos de control de la información tratada), así como las circunstancias y supuestos en los que se permite dicha inclusión. Ello debería articularse en el marco de los principios de legitimación del tratamiento contenidos en el artículo 7 de la Directiva 95/46/CE.

- Actualizar la información. Sería de gran importancia tratar de definir parámetros generales que permitan uniformizar plazos de conservación o bloqueo de los datos contenidos en los ficheros. La falta de transparencia en relación con este principio de calidad de datos consagrado en la Directiva puede conducir a una absoluta indefensión del afectado, debido a la inexistencia de mecanismos que a posteriori puedan subsanar el daño causado (es decir, en supuestos de comunicación de datos a terceros sin el conocimiento del afectado). Habría que eliminar las diferencias de criterio existentes en la actualidad en los Estados miembros, y facilitaría la labor de los operadores económicos en el marco del derecho de la competencia, en línea con lo dispuesto en el considerando 7 de la Directiva 95/46/CE.

- Establecer claramente el derecho del interesado a ser informado acerca del tratamiento de sus datos personales en estos ficheros o listas. Cuando se viola este principio capital, se produce una total indefensión del ciudadano, ya que ni siquiera tiene conocimiento del registro de sus datos personales en una lista negra al no ser él la fuente de los mismos, lo que le impide el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición.

- Regular el procedimiento de notificación al afectado, con inclusión de criterios de información en tiempo y forma. Y establecer una clara indicación de las condiciones, en su caso, para que pueda procederse a su comunicación a terceros.

- Articular mecanismos que incluyan la información que se da al afectado al denegársele un determinado servicio y, en su caso, posibilidades de comprobación y verificación ulteriores por parte del mismo (en el marco de las garantías anteriormente aludidas). De hecho, la Directiva reconoce el derecho del interesado a no verse sometido a una decisión con efectos jurídicos que le afecte de manera significativa y que se base únicamente en un tratamiento automatizado de datos destinados a evaluar aspectos de su personalidad.

- Establecer mecanismos que posibiliten la intervención del afectado, así como la posibilidad de que, de forma motivada y ante supuestos litigiosos, pueda solicitar la inclusión en el fichero de la oportuna información que acredite su posición al respecto.

Otro punto fundamental de máxima importancia en supuestos de ficheros centralizados, comunes y compartidos, es el del establecimiento y aplicación de las medidas de seguridad técnicas y de organización adecuadas, así como las condiciones de acceso a los mismos, obligaciones que recaen en el responsable del tratamiento.

Para concluir, dada la trascendencia de este problema, y teniendo en cuenta que existen sectores económicos cruciales (por ejemplo, sector financiero o de telecomunicaciones) en los que la existencia de este tipo de ficheros afecta a un importante número de ciudadanos, el GT29 desea concienciar a las instituciones comunitarias acerca de la necesidad de avanzar en la línea marcada por las anteriores conclusiones y destacar la necesidad de que en este ámbito existan criterios comunes, directrices o líneas de actuación, en el marco de y de conformidad con la Directiva 95/46/CE y con las respectivas legislaciones internas de los Estados Miembros.

1.5. Análisis de la existencia de un nivel adecuado de protección en terceros Estados

El Gobierno de la República Argentina solicitó a la Comisión que determinara si dicho país garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el artículo 25 de la Directiva. Para poder considerar esta petición la Comisión Europea solicitó el pronunciamiento del GT29 al respecto.

Los criterios y requisitos que el GT29 estima necesarios con el fin de analizar, apreciar y determinar acerca de la existencia de un nivel de protección de datos adecuado en no miembros de la Unión Europea, se contienen en el Documento de Trabajo sobre Transfe-

rencias 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 (ver WP 12).

Básicamente, los objetivos de un sistema de protección de datos, y los estándares de calidad que debe ofrecer la legislación de un estado para ser considerado como adecuado, son:

- 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 2002, el GT29 se ha pronunciado favorablemente en relación con el nivel de protección otorgado por la Ley sobre protección de datos personales de Argentina, de 4 de octubre de 2000 (ver WP 63). Conviene subrayar que la Agencia española ha colaborado intensivamente con el Ministerio de Justicia de aquél país prestando su asesoramiento, apoyo y experiencia en la elaboración de dicha norma legal.

También hay que señalar que, posteriormente, el Comité del Artículo 31 ha votado favorablemente la propuesta de Decisión de la Comisión Europea otorgando dicho *status* a la República Argentina por lo que, si el Parlamento Europeo no presenta ninguna objeción en el plazo legal de que dispone el Parlamento Europeo para revisar el Proyecto de Decisión de la Comisión, se producirá la aprobación formal de la misma y su publicación en el Diario Oficial de la UE.

Conviene recordar finalmente que hasta la fecha y mediante este procedimiento, sólo se ha reconocido la existencia de un nivel adecuado de protección en Hungría, Suiza, Canadá y el Acuerdo de Puerto Seguro.

1.6. Análisis sobre la aplicación del denominado «Acuerdo de Puerto Seguro» con los Estados Unidos de Norteamérica

Ante la próxima conclusión del primer período de dos años de aplicación de la Decisión de la Comisión de 26 de julio de 2000 relativa al acuerdo de *Puerto Seguro,* el GT29 ha considerado necesario empezar a examinar el estado de aplicación de dicho acuerdo (ver WP 62).

Tras recabar información de las distintas autoridades europeas y de los Estados Unidos, encargadas de la aplicación del Acuerdo, así como de las asociaciones afectadas, el GT29 invita a mejorar ciertos aspectos, promoviendo una serie de medidas necesarias para el buen funcionamiento del mismo, y así cita expresamente:

- medidas para aumentar la transparencia de las entidades signatarias, especialmente si la declaración de adhesión al Acuerdo de Puerto Seguro no va acompañada de políticas de privacidad adecuadas;

- prever mecanismos suplementarios de verificación respecto al procedimiento de adhesión al Acuerdo, el cumplimiento de las políticas de privacidad por parte de las entidades que lo han suscrito el acuerdo de puerto seguro y la posible pérdida de los beneficios del mismo;

- dar a conocer mejor los requisitos previos para la adhesión a los principios de puerto seguro, también mediante documentos breves y fácilmente comprensibles y la posible integración del *Safe Harbor Workbook;*

- medidas para perfeccionar los mecanismos de resolución de litigios, mejorar la uniformidad y publicidad de los criterios pertinentes, aumentar la transparencia de los resultados de los litigios y racionalizar sus mecanismos de publicación;

- resolver las dificultades que pueden derivarse de la existencia de múltiples políticas de privacidad declaradas por el mismo operador;

- y medidas destinadas a renovar la cooperación entre el Panel europeo de protección de datos, los organismos responsables de la resolución de litigios y la Comisión Federal de Comercio (FTC).

Además, y aunque no se hayan aprobado documentos concretos relativos a esta materia, hay que hacer constar el importante trabajo realizado por otro Subgrupo en el que desde su fundación participa intensamente la APD. Nos referimos al Subgrupo de Cláusulas que, durante el año 2002, inició el estudio de un modelo de cláusulas contractuales tipo presentadas por un Grupo de Empresas de ámbito internacional, lideradas por la Cámara Internacional de Comercio. Tras haber producido varios informes presentados y aprobados por el GT29, en la actualidad la propuesta se encuentra aún pendiente de determinar varios puntos que son decisivos para poder cerrar la discusión y matizar algunos aspectos adicionales. El Subgrupo de Cláusulas Contractuales inició, además, el estudio, en el ámbito de transferencias internacionales a terceros países, de las Reglas Corporativas Vinculantes entre grupos de empresas, tema que por su novedad y los interrogantes jurídicos que plantea, se ha seguido discutiendo y, probablemente, se producirá la aprobación de un documento sobre la materia en el próximo año.

1.7. La vigilancia de las comunicaciones electrónicas en el lugar de trabajo

Otro importante documento del GT29, aprobado en mayo de 2002, examina la cuestión de la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo, o, dicho de otro modo, la vigilancia por el empleador de la utilización del correo electrónico e Internet por los trabajadores[5].

En él se analiza la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, otros textos internacionales pertinentes y la Directiva 95/46/CE, y se ofrece una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empleador.

Se parte de una reflexión inicial, los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Por el contrario, esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores.

Para equilibrar los distintos derechos e intereses es preciso tener en cuenta varios principios, en particular, el principio de proporcionalidad. Debe quedar claro que el mero hecho de que una actividad de control o vigilancia se considere útil para proteger el interés del empleador no justifica la intromisión en la vida privada del trabajador. Antes de aplicar en el lugar de trabajo cualquier medida de vigilancia, deben sopesarse una serie de aspectos que se detallan en el propio informe.

De las recomendaciones que se contienen en este documento, se puede subrayar la importancia de que el empleador informe al trabajador de la presencia, utilización y objetivo de todo equipo o aparato de detección activado en su puesto de trabajo, así como de cualquier abuso de las comunicaciones electrónicas detectado (correo electrónico o Internet), salvo si existen razones imperiosas que justifiquen la continuación de la vigilancia encubierta, lo que normalmente no sucede.

---

[5] Puede consultarse su texto íntegro, como WP55, del año 2002, en la dirección: http://www.europa.eu.int/comm/privacy

La información sobre la existencia de todas estas medidas puede transmitirse rápida y fácilmente mediante un programa informático, por ej. ventanas de advertencia que avisen al trabajador de que el sistema ha detectado y/o tomado medidas para evitar una utilización ilícita de la red.

El GT29 apunta como solución práctica, que los empleadores consideren la posibilidad de proporcionar a los trabajadores dos cuentas de correo electrónico:

a) una de uso profesional exclusivo, en la que se permitiría un control dentro de los límites detallados en el Documento de Trabajo,
b) otra de uso estrictamente privado (o con autorización de utilizar el correo *web*), que sólo sería objeto de medidas de seguridad y que se controlaría para prevenir abusos en casos excepcionales.

Uno de los mayores esfuerzos en la redacción de este Documento fue tratar de hacerlo compatible con todas las legislaciones de los Estados miembros, donde en ocasiones, la propia ley nacional puede prever un nivel de protección más elevado que el que se contempla en él.

Todas las recomendaciones que se contienen en el mismo pueden orientar eficazmente a los responsables, a la hora de organizar el acceso y la utilización de los medios electrónicos por parte de sus empleados, en el lugar del trabajo.

Por último, además de en las labores preparatorias del Documento antes comentado, en el Subgrupo de Datos de Empleo se iniciaron trabajos dirigidos a valorar el Código de conducta presentado por la Asociación de búsqueda de Asesores Ejecutivos (AESC – Association of Executive Search Consultants, Europe) para el tratamiento de datos personales. En estos momentos las discusiones y encuentros con representantes de dicha Asociación continúan para aclarar determinados aspectos de los documentos presentados.

2. Consejo de Europa

2.1. Introducción

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) del Consejo de Europa, es primer instrumento internacional que vincula a los Estados signatarios del mismo para adoptar la legislación nacional necesaria que introduzca en su Derecho interno principios y garantías relativos a la protección de datos personales. Fue abierto a la firma en 1981 y ratificado por España en 1985.

A continuación se dará cuenta de las actividades principales llevadas a cabo durante el año 2002 en el marco del Consejo de Europa en relación con distintos aspectos de desarrollo del Convenio 108.

2.2. Reuniones del Grupo de Proyectos de Protección de Datos

El Convenio 108 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 igualmente del cumplimiento del Convenio.

Asimismo, dado que los principios contenidos en el Convenio deben adaptarse e interpretarse en función de los diferentes sectores implicados en el tratamiento de la información personal, el Consejo de Europa ha aprobado distintas Recomendaciones dirigidas a dichos sectores. 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.

En octubre del año 2002 se celebró una reunión del CJ-PD, habiéndose mantenido con anterioridad una reunión preparatoria del Grupo de Coordinación del mismo (CJ-PD-GC), asistiendo representantes de la Agencia a ambas.

Dentro de la actividad de este Comité, podemos destacar la aprobación del borrador de los informes sobre *«Principios orientadores relativos a la protección de personas en relación con la obtención de tratamientos de datos por medios de videovigilancia»* y sobre el *«Impacto de los principios de protección de datos en las actividades judiciales y policiales»*, habiendo sido ambos aprobados por el Comité Europeo sobre Cooperación Jurídica, órgano competente del Consejo de Europa a estos efectos[6].

2.3. Recomendación para la protección de datos recogidos y tratados para fines relacionados con el sector del seguro

En Memorias anteriores ya se dio noticia de la elaboración en el ámbito del Consejo de Europa de un Proyecto de Recomendación referente al tratamiento de los datos personales

[6] Ambos textos se pueden consultar en http://www.coe.int/dataprotection

relacionado con las distintas modalidades de tratamiento de datos de carácter personal relacionadas con el sector asegurador.

La Recomendación fue finalmente aprobada por el Comité de Ministros del Consejo de Europa en su sesión de 18 de septiembre de 2002, bajo la denominación *«Recomendación Nº R (2002) 9 sobre la protección de los datos de carácter personal recogidos y tratados para finalidades relacionados con los seguros»*, que a continuación se resume brevemente[7]:

Respecto de su ámbito de aplicación, la Recomendación será de aplicación a la recogida y tratamiento de datos para finalidades relacionadas con seguros, quedando excluidas las actividades relacionadas con la seguridad social, sin perjuicio de que los Estados puedan extender la aplicación de la Recomendación a dichas actividades. Asimismo se prevé la posibilidad de extender los efectos de la Recomendación a datos no automatizados y a personas jurídicas.

En relación con los fines, tal y como se indica en el apartado 4.4 de la Recomendación, los datos podrán ser objeto de tratamiento con la finalidad de la preparación y celebración de un contrato, la cuantificación de las primas, el pago de indemnizaciones, el reaseguro, el coaseguro, la prevención del fraude, la resolución de quejas, el cumplimiento de otras obligaciones legales o contractuales, la prospección de nuevos mercados, la gestión interna y la realización de actividades actuariales. En todo caso, los datos no podrán ser utilizados para fines incompatibles con los que motivaron su recogida.

El tratamiento de datos sensibles se encuentra prohibido a menos que el afectado, o su representante si carece de capacidad, hubieran dado su consentimiento, si se efectúa para el cumplimiento de una función relacionada con el interés público o si se permite por la Ley, dada la naturaleza de la actividad y previa la adopción de las debidas garantías de seguridad.

Del mismo modo, el tratamiento de datos relacionado con actividades criminales será posible en los supuestos en que así lo permita la Ley interna y los datos tengan por objeto evitar actividades de fraude por parte del afectado.

Por otro lado, la persona cuyos datos son objeto de tratamiento deberá ser informada, antes de dicho tratamiento, si los datos se recogen de él o, en caso contrario, antes de ser comunicados a un tercero, de las categorías de datos recogidos, las finalidades del tratamiento, la identificación del responsable del tratamiento, el modo de ejercicio de los derechos de acceso y rectificación, las categorías de personas destinatarias de los datos, el carácter obligatorio o facultativo de facilitarlos o, en su caso, las consecuencias derivadas de no hacerlo.

---

[7] El texto íntegro de la Recomendación y su Memoria Explicativa pueden consultarse en el sitio web http://www.coe.int/dataprotection

Esta obligación sólo se verá exceptuada si el interesado ha sido previamente informado, si la Ley interna lo permite o si el hacerlo encierra un esfuerzo desproporcionado.

Por su parte, el consentimiento deberá ser libre, específico, informado, inequívoco y, en caso de datos sensibles, expreso. Además deberá ser dado por el propio afectado salvo que carezca de capacidad legal para ello, en cuyo caso, corresponderá otorgarlo a su representante legal.

En el caso de tratamientos por terceros por cuenta del responsable, la relación entre ambos deberá estar regida por un contrato u otro instrumento vinculante para el encargado, que sólo podrá actuar dentro de los límites que establezca el responsable del tratamiento o la Ley interna. Además, la Recomendación prevé que el encargado deberá ofrecer medidas de seguridad adecuadas, tanto desde el punto de vista técnico como desde el organizativo que permitan, entre otras cosas, asegurar que el tratamiento sólo se desarrolla en el marco de las instrucciones del responsable.

Los datos sólo podrán ser utilizados para las finalidades anteriormente descritas. Cualquier otro uso requerirá que la Ley lo prevea expresamente o que el afectado haya prestado su consentimiento, que deberá ser expreso si se trata de datos especialmente sensibles.

No obstante se permite la utilización para fines de marketing directo si el interesado no se opone a ello. Del mismo modo, será posible el tratamiento para el cumplimiento de fines legítimos del asegurador si no prevalece sobre ellos el interés del asegurado.

Si bien se prevé que, con carácter general, no será posible la adopción de decisiones basadas exclusivamente en los datos tratados, se permite la adopción de las mismas cuando los datos hayan sido facilitados por el afectado con la intención de celebrar un contrato de seguro, en orden a establecer sus términos.

En caso de que así lo soliciten, los afectados tienen derecho a conocer, de forma inteligible, los datos que han sido tratados, las finalidades para las que se tratan, los destinatarios de dichos datos y las fuentes de donde se obtuvieron en caso de que no sean el propio interesado. Este derecho sólo podrá restringirse en caso de prevención, investigación o persecución de delitos o en garantía de derechos de terceros, y sólo mientras no desaparezca esta causa.

Por otra parte, los afectados tienen derecho a obtener la rectificación, bloqueo o cancelación de los datos que sean inadecuados, irrelevantes o excesivos respecto a la finalidad que motiva su tratamiento, debiendo informarse de estas circunstancias a los terceros a los que hayan sido cedidos los datos.

La Recomendación detalla las medidas técnicas y organizativas que deberán adoptarse para proteger los datos objeto de tratamiento, siempre de acuerdo con los criterios que se establezcan por las legislaciones nacionales de los Estados miembros.

Para las transferencias de datos personales a terceros países, regirán los principios generales del Convenio 108. Ello supone que, con carácter general, será libre la transferencia a otros países signatarios del citado Convenio que ofrezcan un nivel de protección equivalente al previsto en el mismo. En caso de terceros estados no signatarios sólo será posible la transferencia cuando el interesado lo haya consentido o si se ofrecieran garantías adecuadas, incluidas las de naturaleza contractual en su caso.

Finalmente, los datos deberán ser eliminados cuando dejen de ser necesarios para el cumplimiento de los fines que motivaron su recogida, incluido el caso en que se rechace la celebración del contrato por parte de la compañía aseguradora, a menos que se conserven para fines estadísticos y previa la necesaria disociación.

Las legislaciones nacionales adoptarán medidas a fin de regular las compensaciones e indemnizaciones que sean procedentes como consecuencia del incumplimiento de la Recomendación.

2.4. Protocolo Adicional al Convenio 108

En noviembre del año 2001 como ya se especificó en la Memoria anterior, se abrió a la firma el Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a las Transferencias Internacionales de Datos. Durante el año 2002 cinco nuevos Estados procedieron a su firma: Bélgica, Chipre, República Checa, Polonia y Suiza, habiendo sido ratificado en ese mismo año por Eslovaquia. Por ello, en estos momentos son ya veintitrés los Estados que lo han firmado, habiendo sido ratificado por Grecia, Eslovaquia y Suecia.

2.5. Conferencia de Madrid. Remisión

En el mes de diciembre de 2002, la APD y el Consejo de Europa organizaron conjuntamente una Conferencia sobre los retos a los que deben enfrentarse las autoridades de protección de datos recientemente establecidas, que, por su especial relevancia, se trata separadamente en un epígrafe específico de esta Memoria.

3. Autoridad de Control Común del Sistema de Información Schengen

El Convenio de Aplicación del Acuerdo de Schengen se ha configurado como el precursor del espacio de libertad, seguridad y justicia creado por el Tratado de Ámsterdam que, además, establece la plena incorporación del Convenio de Aplicación del Acuerdo de Schengen al Acervo Comunitario. El éxito de este Acuerdo es absoluto si se tiene en cuenta que de los cinco países que lo firmaron inicialmente en 1990 se ha pasado en la actualidad a quince (Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal y Suecia).

Hay que recordar que el objetivo del Acuerdo de Schengen y su Convenio de Aplicación es la supresión de los controles en las fronteras interiores de los Estados miembros, creando con ello un gran espacio de libre circulación de personas. Con el fin de alcanzar este objetivo al tiempo que se mantiene en dicho espacio un nivel de seguridad por lo menos igual al que existía anteriormente, el Convenio de Aplicación del Acuerdo de Schengen establece una serie de medidas compensatorias. Entre estas medidas figuran, principalmente, la armonización de la política en materia de expedición de visados, la creación de una política común en materia de determinación del Estado responsable del examen de una solicitud de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico de estupefacientes, la armonización del nivel de control de las fronteras exteriores del espacio 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 aquellos 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 cinco sesiones plenarias que ha celebrado la ACC durante el año 2002 en la sede del Consejo de la Unión Europea en Bruselas. A continuación se presentan algunos de los temas tratados por la ACC durante el pasado año.

3.1. Inclusión de nuevas funcionalidades en el SIS

Uno de los principales trabajos realizados por la ACC durante el pasado año ha sido el análisis de las propuestas que se han venido presentando para añadir nuevas funcionalidades al SIS, encontrándose principalmente entre éstas una Iniciativa española que, con vistas a la adopción de una Decisión y Reglamento del Consejo, pretende añadir nuevas funcionalidades en particular en materia de lucha contra el terrorismo. Esta iniciativa se está modificando en función de los comentarios que se vienen realizado desde los diferentes Grupos de Trabajo del Consejo.

Entre las modificaciones que se han propuesto se encuentran: facilitar a las Oficinas SIRENE una regulación jurídica que justifique su existencia y que hasta la fecha no se contemplaba en el Acervo de Schengen; inclusión de nuevos elementos de información en relación con las personas incluidas en el SIS, autorizar el acceso al SIS a las autoridades judiciales, a la Oficina de Policía Europea (EUROPOL) y a los miembros nacionales de EUROJUST y la modificación del periodo de mantenimiento de la información que se registra en relación con las consultas realizadas al SIS.

La ACC se ha pronunciado en diferentes ocasiones en relación con esta Iniciativa, a medida que la misma se ha ido modificando. En sus dictámenes la ACC ha solicitado que se justifique con mayor rigor la necesidad de la inclusión de las nuevas categorías de datos para personas, así como la concesión a EUROPOL y EUROJUST de acceso a determinados datos del SIS. Respecto de la creación de una regulación jurídica a las Oficinas SIRENE ha mostrado su satisfacción por cuanto ello había sido requerido por esta Autoridad en numerosas ocasiones, pero solicitaba la inclusión de reglas adicionales que definieran el uso que estas Oficinas pudieran hacer de los datos del SIS, con el fin de que se limitara a las finalidades ya estipuladas en el Convenio. En relación con la ampliación del plazo a tres años -en la actualidad es de seis meses- de la información registrada sobre las consultas realizadas al SIS, la ACC ha considerado que tal ampliación no es proporcional con la finalidad para la que se mantiene esta información, que no es otra que la verificación a posteriori de la admisibilidad de las consultas que se hayan efectuado.

3.2. Vademécum relativo al ejercicio del derecho de acceso

En el pasado año la ACC finalizó los trabajos relativos a la elaboración de un vademécum cuyo objeto es describir las modalidades de ejercicio del derecho de acceso al SIS. Esta guía contempla tres apartados: una recapitulación de los principios generales y de las definicio-

nes esenciales relativas al SIS, una descripción del procedimiento de ejercicio del derecho de acceso en cada uno de los países interesados y una presentación de algunas situaciones particulares que requieren un procedimiento específico.

En el primer apartado se presentan los derechos en materia de protección de datos que el Convenio de Schengen otorga a las personas, sean o no nacionales de un Estado miembro del espacio de Schengen: el derecho de acceso a las informaciones que se refieran a ellas y estén introducidas en el SIS, el derecho de rectificación cuando los datos contengan errores de hecho o de derecho y el derecho de emprender acciones ante el órgano jurisdiccional o la autoridad competente a efectos de rectificación o supresión de datos erróneos o de indemnización. Asimismo, se presentan las modalidades de ejercicio de derecho de acceso existentes: directo (la petición se dirige directamente al responsable del fichero) e indirecto (la petición debe remitirse a la autoridad nacional de protección de datos).

En el segundo apartado se presenta información del procedimiento que debe seguirse en cada uno de los países que aplican el Acervo de Schengen para ejercer el derecho de acceso, detallándose en cada caso: modalidad de ejercicio del derecho de acceso, dirección del organismo al que dirigirse, información y documentación que debe facilitarse, dirección de la autoridad nacional de control, resultados que cabe esperar de la solicitud y referencias de los principales textos legales aplicables.

En el tercer apartado se recogen las directrices que deberían seguir las autoridades nacionales de control y diversas consideraciones a tener en cuenta, en relación con tres situaciones particulares: principios de cooperación entre estas autoridades, registros de alias y descripción de un extranjero titular de un permiso de residencia expedido por un Estado miembro.

La primera situación se produce cuando una persona dirige su solicitud de acceso a una autoridad nacional de control de un determinado Estado miembro del espacio Schengen y la descripción ha sido introducida por otro diferente; la ACC considera que deberá establecerse una estrecha cooperación entre las autoridades de control de los dos Estados afectados: el Estado en el que se presenta la solicitud de acceso y el Estado que procedió a la descripción. En la segunda situación se describen los problemas jurídicos y prácticos que se presentan en aquellas descripciones del SIS de personas cuya identidad ha sido usurpada, es decir, el registro de personas concretas que no mantienen ninguna relación con la identidad de la persona que realmente se busca. Por último, la tercera situación se produce cuando se comprueba que un extranjero titular de un permiso de residencia válido, expedido por Estado miembro, está incluido como persona no admisible en el SIS; situación que de conformidad con el Convenio debería iniciar un procedimiento de consulta entre los países, cuyo resultado final debiera ser la retirada de dicha descripción del SIS.

3.3. Mantenimiento de las descripciones de personas no admisibles

La Autoridad de Control griega solicitó a la ACC un dictamen acerca del periodo en que debían conservarse los datos de las personas consideradas como no admisibles incluidas al amparo del artículo 96 del Convenio de Schengen y, en concreto, si debía aplicarse para su revisión y supresión lo estipulado en el artículo 112 o en el 113, lo que supondría en el primer caso un periodo de conservación de tres años y de diez en el segundo. La Autoridad de Control griega planteaba inicialmente que debía aplicarse uno u otro, en función de la acción que se fuera a emprender a propósito de la descripción.

En su Dictamen la ACC considera que de conformidad con lo estipulado en el Convenio, el SIS contiene datos que, con motivo del control de una persona, permiten que las autoridades comprueben si dicha persona ha sido objeto de una descripción y, si así fuera, informar acerca de la acción específica que se deberá emprender. Aunque los fines de las descripciones pueden ser diversos, la función del SIS es la misma para todas ellas: alertar a las autoridades de la necesidad de una determinada acción. Asimismo, se considera que ni el Convenio de Schengen ni el SIS establecen distinciones entre los diferentes tipos de acción policial.

Por ello y, teniendo en cuenta que el artículo 112 contiene disposiciones para la revisión y supresión de datos personales registrados en el SIS a efectos de búsqueda de personas, la ACC resuelve que este artículo es el único que determina el período de revisión y supresión de los datos personales que se registran en el SIS.

3.4. Implementación del SIS en el Reino Unido e Irlanda

Mediante una Decisión de 29 de mayo de 2000, el Consejo acordó que tanto el Reino Unido de Gran Bretaña como Irlanda participaran en algunas de las disposiciones del acervo de Schengen, pero esta participación no incluía las disposiciones relativas al SIS que se refieran al artículo 96, de personas no admisibles en el territorio Schengen.

El problema que se planteaba era de índole jurídica y técnica, por cuanto el Convenio de Schengen venía configurado bajo el principio básico de cooperación completa entre todos los países participantes, situación que claramente quedaba modificada con esta nueva modalidad de participación del Reino Unido e Irlanda.

Uno de los principales escollos fue determinar si estos países debían disponer de la totalidad de la base de datos del SIS, incluyendo también los relativos al artículo 96. Desde el primer momento la ACC mostró su oposición a esta solución, por cuanto consideraba que ello contravendría lo dispuesto en el Convenio respecto de las garantías que se imponen respecto del acceso y uso de los datos del SIS. La solución técnica adoptada finalmente excluía que los datos relativos al artículo 96 se enviaran a estos países, estableciéndose un procedimiento de filtrado de los mismos en el propio CSIS así como mecanismos para la detección de descripciones duplicadas de personas que no implicasen la transmisión de estos datos al Reino Unido e Irlanda.

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)[8], 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 con-

[8] Tanto el Convenio Europol como el resto de la normativa reguladora de Europol puede encontrarse en http://www.europol.eu.int

seguir 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 policía[9].

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 seis ocasiones en el transcurso de 2002. 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 plenario[10]. Debe destacarse que en la reunión de la ACC-Europol de octubre de 2002 se eligió nuevo presidente y vicepresidente, recayendo este último nombramiento en uno de los miembros de España en la ACC-Europol.

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 necesario[11]. Como novedad importante a este respecto, cabe destacar que en junio de

---

[9] Véase el artículo 14 del Convenio Europol.

[10] Para una descripción detallada de estos subgrupos, consultar la Memoria correspondiente al ejercicio de 2000. En el año 2002 han sido los Subgrupos de Acuerdos internacionales (también denominado de «Procedimientos); de Órdenes de Creación de Ficheros de Análisis, Inspección y Nuevas Tecnologías los que se han mantenido operativos y han procedido al estudio y ejecución de los trabajos y tareas que el Plenario les ha encomendado. Así mismo, debe destacarse que en diciembre de 2002 se constituyó un Subgrupo de Trabajo en el seno de la ACC-Europol encargado del estudio de los sistemas de bases de datos y ficheros previstos en el Convenio Europol, en el marco del estudio sistemático de las bases de datos establecidas en los Convenios del Tercer Pilar (Schengen y Sistema de Información Aduanero).

[11] 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.

2002 se acordó en el seno de la ACC-Europol, con objeto de agilizar el procedimiento de emanación del dictamen preceptivo, y a través del oportuno mandato, que el Subgrupo de trabajo sobre disposiciones de creación pueda elaborar un dictamen en nombre de la ACC-Europol en aquellos casos en los que la disposición de creación se refiera a un tema de análisis concreto sobre el que la ACC-Europol haya evacuado el oportuno dictamen en el pasado. Si alguna de las delegaciones desea solicitar un debate plenario al respecto, deberá hacerlo en el plazo de los cinco días siguientes a la distribución de la disposición de creación. En este supuesto, el Subgrupo deberá preparar un dictamen Plenario en el seno de la ACC-Europol.

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 mismas[12]. En el año 2002 se han emitido dictámenes favorables al inicio de negociaciones con Canadá, Bulgaria, República de Eslovaquia, Lituania, Letonia y Chipre.

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 mismos[13]. En este sentido, la ACC-Europol ha emanado dictámenes favorables a los Proyectos de Acuerdo celebrados con Estados Unidos así como con Bulgaria, República de Eslovaquia y Chipre.

En el Dictamen aprobado por la ACC-Europol en octubre de 2002 y relativo al Acuerdo entre Europol y Estados Unidos, se señala la inexistencia de obstáculos para que el Consejo autorice al Director de Europol la firma del Acuerdo, si bien se destacan una serie de aspectos que deberían ser tenidos en consideración en un intercambio de cartas clarificador de los puntos más controvertidos (principio de finalidad en relación con los datos transmitidos y tratados, obligatoria sujeción a la letra del art. 18 del Convenio Europol, supervisión en la ejecución del Acuerdo y seguimiento de la aplicación del mismo y del intercambio de cartas suscrito al efecto, entre otros).

Otro hecho importante ha sido el otorgamiento de mandato al Subgrupo de Inspección formado en el seno de la ACC-Europol para la realización de la segunda inspección. En junio de 2002 se efectuó la segunda auditoria y se produjo la aprobación del texto definitivo del

---

[12] 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.

[13] 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.

Informe de Inspección elaborado por el equipo de expertos que realizaron la misma -que contaba con un Inspector de la Agencia de Protección de Datos- tras tener en cuenta los comentarios realizados por Europol. Dicho Informe respondía a los objetivos de comprobar la efectiva implantación de las recomendaciones realizadas en el primer Informe de Inspección (octubre de 2001), del que se informó en la Memoria del año pasado, así como profundizar en el conocimiento y operativa del Sistema de Análisis y verificar el nuevo Sistema de Información cuya implantación tiene prevista Europol. 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.

Así mismo, en el transcurso del pasado año se circuló por parte de la Secretaría de la ACC-Europol un cuestionario sobre protección de datos y ficheros policiales que fue cumplimentado por las distintas delegaciones y cuyas contribuciones se incorporaron en un único documento redistribuido posteriormente. Dicho cuestionario se estructuraba en tres apartados, a saber: Régimen jurídico aplicable en materia de protección de datos a los ficheros policiales; Su relación con la competencia de Europol y papel de las Autoridades de Control en relación con dichos ficheros.

Una cuestión de capital importancia que se inició en el transcurso de 2002 (con Presidencia danesa) y cuya conclusión se materializará presumiblemente (con Presidencia griega) en 2003, es la modificación del Convenio Europol.

La ACC-Europol se pronunció en octubre de 2002 sobre la primera propuesta de modificación del Convenio Europol (se han producido dos propuestas de modificación, habiendo sido analizada la segunda por parte de la ACC-Europol en marzo de 2003, por lo que se dará cumplida información al respecto en la próxima Memoria).

La primera propuesta de modificación del Convenio trataba cuestiones sobre las que se pronunció la ACC-Europol ya que afectaban a la actividad, cometidos y funciones de la ACC-Europol en el marco de las competencias que le atribuye el Convenio Europol.

Dichas cuestiones se referían al objetivo, finalidades y funciones de Europol; competencias de las Unidades nacionales; derecho de acceso al sistema de información; recogida, tratamiento y utilización de datos personales; procedimientos de apertura o disposiciones de creación de ficheros; normas de constancia documental; transmisiones de datos a organismos terceros, plazos de conservación y supresión de ficheros.

En la actualidad, y tras la presentación de una segunda propuesta de modificación del Convenio Europol, informada por la ACC-Europol tras su reunión de marzo 2003, aún no se ha producido aprobación de dicha modificación. Se dará cumplida información de los avances que se produzcan en la Memoria correspondiente a 2003.

Otro aspecto de gran relevancia tratada por la ACC-Europol en el transcurso del año 2002 es el de posibilitar la participación de los diez candidatos a la adhesión a la Unión Europea en próximas reuniones de la ACC-Europol. Los representantes de dichos Estados participaron como observadores en una reunión de la ACC-Europol en el pasado año 2002 y se prevé que puedan formar parte en próximas reuniones de la ACC-Europol con el estatuto de observadores hasta su plena incorporación en la UE.

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 o verificación (artículo 19. 7 del Convenio) o de rectificación y cancelación (artículo 20. 4 del Convenio) de los datos de carácter personal. En el transcurso de 2002, el Comité se reunió en 4 ocasiones.

En el mes de mayo del pasado año 2002, el Comité de Recursos ha resuelto uno de los procedimientos que se encontraban pendientes de resolución y ha continuado la tramitación del segundo y último procedimiento abierto hasta el momento, del que se informará en la próxima Memoria.

El Recurso mencionado, 1/01, tiene origen en la queja presentada por un ciudadano británico que ejercitó su derecho de acceso solicitando a Europol que le remitiese información sobre posibles datos personales suyos que estuviesen almacenados en sus registros. Europol respondió 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». El interesado acudió al Comité de Recursos recurriendo la respuesta de Europol. Tras admitir la denuncia a trámite, procedió a dar curso y cumplimiento a las fases procedimentales previstas en el Reglamento (DOCE C 149/3 de 28 de mayo de 1999) de la Autoridad Común de Control de Europol, arts. Arts. 11 a 28. La decisión del Comité de Recursos se produjo en mayo de 2002, considerando que la decisión de Europol se ajusta al Convenio Europol, arts. 19 (3) y (5).

Por su parte, cabe señalar que el Recurso 2/02 obedece a una denuncia presentada por un ciudadano de origen griego residente en Países Bajos. Este recurso se encuentra actualmente en la última fase del procedimiento, y, por tanto, pendiente de resolución.

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 con base en el 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)[14].

El Convenio SIA, siguiendo la estructura del resto de instrumentos legales existentes en el marco del III Pilar, crea una Autoridad de Supervisión Común[15], 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

[14] 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/index.html

[15] Véase el apartado 1 del articulo 18 del Convenio SIA.

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, y 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 finales de 2001 a la aprobación provisional y por unanimidad, del Proyecto de Reglamento, que ha sido formalmente aprobado en 2002, año en el que la ASC-SIA ha mantenido cuatro reuniones. La delegación española, además de valorar y participar en las discusiones en las distintas reuniones en las que se trató la propuesta de Reglamento, solicitó expresamente la inclusión de la normativa comunitaria en vigor respecto del apartado relativo al acceso del público a los documentos de la ASC-SIA, ya que a pesar de contener la práctica totalidad de los distintos supuestos, había una parte que no se había reflejado en el Reglamento.

En el transcurso de 2002 se ha procedido así mismo a la elección por unanimidad del Presidente (miembro de la Autoridad del Reino Unido) y Vicepresidente (miembro de la Autoridad de Italia) de la ASC-SIA.

Así mismo, se han tratado con el Presidente del Grupo de Trabajo de cooperación Aduanera temas relativos al desarrollo y puesta en marcha del Sistema de Información Aduanero (conocido como CIS – *Customs Information System*) previsto en el Convenio SIA, aspecto en el que también se encuentra involucrada la Oficina Antifraude de la Comisión Europea, ya que es posible que aporte presupuesto para el desenvolvimiento operativo de un plan de actuación de desarrollo del CIS. Dicho Plan se tradujo en el Borrador de Manual de Procedimientos del Sistema de Información Aduanero, presentado por la Oficina Antifraude, integrada en la Dirección General de Asuntos Jurídicos y Legislativos de la Comisión Europea y cuya finalidad es la de otorgar ayuda práctica desde el punto de vista técnico y operativo-procedimental, basado, por lo tanto, en cuestiones fundamentalmente técnicas y respecto del que la ASC-SIA no planteó objeciones.

A finales del pasado año 2002 la ASC-SIA trató el Proyecto de Protocolo de modificación del Convenio SIA, que introduce una base de datos relativa a un fichero de expedientes de investigación aduanera (denominada base de datos FIDE), por lo que el dictamen de la ACC-SIA será emitido en el año 2003. No obstante, puede adelantarse que el punto fundamental que abordará y sobre el que llamará la atención se refiere a las nuevas categorías de datos personales que pueden ser incorporados en la base de datos de identificación CIS.

Debe así mismo destacarse que, al igual que ha sucedido en relación con los Convenios Schengen y Europol, se ha constituido a finales de 2002 en el marco de la ASC-SIA un Grupo de trabajo encargado de iniciar trabajos en relación con un estudio de los bancos de datos creados por parte del Convenio SIA. Del desarrollo de sus trabajos y actuaciones se informará en la próxima memoria.

6. Eurodac

El Reglamento (CE) Nº 2725/2000[16] 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 Dublín[17], 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.

---

[16] Véase http://europa.eu.int/eur-lex/es/index.html para consultar una versión on-line del Reglamento Eurodac

[17] 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/index.html

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.

Dado 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.

Tras producirse estos nombramientos, el 5 de septiembre de 2002 se produjo una reunión informal a la que fueron convocados los representantes de cada uno de los Estados miembros que habían procedido a su nombramiento. Durante la misma, la Comisión Europea informó de la situación del procedimiento para nombrar el primer Supervisor Europeo de

Protección de Datos, que asumirá las funciones de la Autoridad Común una vez nombrado, estimándose un plazo mínimo de seis meses para que todo el proceso pudiera completarse.

A continuación los servicios de la Comisión presentaron otro Informe de situación relativo a la Unidad Central de EURODAC en el que se daba cuenta de los planes existentes para que, tras la finalización de las fases de Análisis y Diseño de los Requerimientos del Sistema, Desarrollo de las Aplicaciones, Instalación de la Unidad Central, Desarrollo de un programa cliente de referencia para los Estados miembros, se anunciara el comienzo de la fase de pruebas para el 6 de diciembre de 2002, siendo la fecha prevista para la entrada en funcionamiento en red para todos los Estados miembros a los que les era de aplicación el Reglamento el 15 de enero de 2003.

También se analizó un primer borrador de Reglamento Interno de la Autoridad Común de Control, sobre el que las delegaciones realizaron distintos comentarios. Se acordó que la Secretaría prepararía un nuevo texto a la luz de las intervenciones habidas en la reunión y lo circularía con el fin de recibir nuevos comentarios de tal manera que para la primera reunión formal de la Autoridad, pudiera procederse a su aprobación.

Así, el día 28 de noviembre de 2002 tuvo lugar la reunión de constitución de la Autoridad Común de Control de EURODAC en la que se aprobó el Reglamento Interno de la misma y se procedió a la elección de Presidente y Vicepresidente, resultando elegidos el Sr. Türk de Francia y la Sra. Kotschy de Austria, respectivamente.

La primera reunión finalizó con una exposición, por parte de los servicios de la Comisión, de las medidas de seguridad existentes en la Unidad Central para garantizar que se cumplen los requerimientos en este sentido establecidos en el Reglamento EURODAC.

7. Grupo de Protección de Datos en Telecomunicaciones (Grupo de Berlín)

Como se indicó en las Memorias de los años anteriores, la Agencia española forma parte del Grupo Internacional de Protección de Datos en Telecomunicaciones *(International Working Group on Data Protection in Telecomunications. IWGDPT)*. Este grupo se creó en 1983, a iniciativa de la autoridad de protección de datos del *Länder* de Berlín, donde tiene su sede, y lo novedoso, frente a otros grupos de trabajo es que agrupa junto a representantes de las autoridades de control de un gran número de Estados, a representantes de organizaciones internacionales públicas y privadas, y a representantes de los sectores industriales implicados. Es un foro de trabajo abierto que pretende debatir sobre las implicaciones del uso de las telecomunicaciones en la esfera privada de los individuos, anticipándose a los problemas que se plantean en la práctica.

En el año 2002, como es habitual, este grupo se reunió en dos ocasiones: en Auckland, Nueva Zelanda, los días 26 y 27 de marzo y en Berlín, el 11 y 12 de noviembre. En la reunión de Auckland se aprobaron cuatro interesantes documentos sobre los temas que se detallan a continuación[18]:

[18] Los textos completos de estos documentos, pueden ser consultados en la siguiente dirección de Internet: http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm.

7.1. «La vigilancia de las telecomunicaciones»

En este Documento el Grupo Internacional de Telecomunicaciones hace algunas reflexiones sobre la desproporción de determinadas medidas (interceptación de las comunicaciones y correspondencia) que son empleadas, en algunas sociedades, a raíz de los sucesos terroristas del 11 de septiembre, indiscriminadamente sin justificación alguna. La utilización de estas medidas de vigilancia de las personas tiene que estar plenamente justificada en la lucha contra el terrorismo y el cibercrimen y no puede ser arbitraria ni tener carácter general.

El Grupo analiza a este respecto la jurisprudencia del Tribunal Europeo de Derechos Humanos y apoya la declaración del Parlamento Europeo recomendando la implantación de un sistema global para la interceptación de las comunicaciones comerciales y privadas de forma uniforme. Básicamente se trataría de establecer un código de conducta universal que deberían seguir todas las autoridades encargadas de la interceptación y que permitiría combinar los fines de investigación con los derechos de los investigados.

7.2. «La privacidad de los niños en la red: el papel del consentimiento paterno»

El Documento analiza más que las condiciones de privacidad en la navegación por Internet de los niños o menores, el consentimiento de los padres cuando estos niños facilitan datos o información a los proveedores de servicios, o bien cuando sus datos van a hacerse públicos en alguna página *web*. El Grupo hace una serie de recomendaciones a los responsables del tratamiento de los casos en los que deben recabar el consentimiento paterno y aquellos otros en los que no lo consideran necesario.

7.3. «El uso de los identificadores únicos en los equipos de telecomunicaciones: el ejemplo del Ipv6»

Se llama la atención aquí sobre los riesgos de esta nueva versión del protocolo de Internet (Ipv6) que permite conexiones estables, manteniendo la misma dirección, incluso cuando el terminal se está moviendo en la red. Esta característica de identificador único puede supo-

ner riesgos para la confidencialidad y seguridad. Asimismo, existe la posibilidad de elaboración de perfiles de los usuarios a partir de la actividad de los mismos. El Grupo invoca los principios generales de protección de datos en el desarrollo esta nueva versión de Internet y pide a los responsables de su puesta en práctica que los tengan presente al desarrollar esta nueva tecnología.

7.4. «Medicina a distancia por Internet»

Esta práctica de la medicina a distancia, vía Internet, está adquiriendo en algunos países un auge importante (principalmente en Nueva Zelanda, donde se desarrolló esta Conferencia). Como las implicaciones de este servicio en el ámbito de la protección de datos personales están fuera de toda duda, el Grupo considera necesario hacer varias recomendaciones a los proveedores de servicios de telemedicina vía Internet en orden a garantizar de manera especial la seguridad de la información que recopilan (cifrar), a informar claramente de sus política de privacidad y asegurar que la información sólo será utilizada con fines médicos y nunca con fines comerciales.

En la siguiente reunión de Berlín no se aprobaron documentos pero se debatieron importantes temas sobre privacidad en el mundo de las telecomunicaciones, de la mayor actualidad.

En primer lugar se realizó un seguimiento de las novedades legislativas en materia de Telecomunicaciones, Internet y Administración electrónica, desarrolladas recientemente por los países asistentes. Un aspecto a destacar fue la controversia creada ante la implantación de la retención obligatoria de los datos de tráfico por los proveedores de redes y servicios públicos de comunicaciones, existiendo una fuerte oposición a ello por parte de los parlamentos de algunos países, como los de Reino Unido y Alemania.

Se debatió también el grave problema que se está suscitando en algunos países con los robos de teléfonos móviles. Para bloquear los móviles robados hay mecanismos asociados a la tecnología GSM, que se activan a requerimiento del legítimo dueño, e inutilizan el teléfono. Esto supone, de facto, la creación de unos ficheros nacionales con datos personales (nombre apellidos del titular, asociados al número denominado IMEI que identifica el terminal móvil), que actualmente no están siendo controlados o regulados por nadie. La autoridad de protección de datos francesa, la CNIL *(Comisión Nacional de Informática y Libertades)*, manifestó su preocupación por este asunto y la necesidad de adoptar una solución común.

Otro asunto de interés tratado en esta reunión fue el problema relativo a las Bases de datos WHOIS de Internet, puntualizándose la conveniencia de modificación de la política de la ICANN *(Internet Coorporation for Asigned Names and Numbers)* en relación con ellas. Las Bases de Datos WHOIS contienen información de las personas de contacto de las empresas que mantienen registrados nombres de dominio y direcciones IP en Internet, figurando incluso datos de particulares en el caso de que el nombre de dominio sea registrado por una persona física. Uno de los principales problemas es que el actual Acuerdo de Acreditación, que el Registrador suscribe con la ICANN para prestar este servicio de registro de nombres de dominio, permite la posibilidad de vender a terceras entidades el acceso masivo a datos de las personas de contacto, para su utilización con fines publicitarios. Otro problema añadido es la propuesta existente de extender las capacidades de búsqueda sobre estas bases de datos, contraria a los fines iniciales previstos para estos ficheros. Por todo ello se acordó que la Secretaría del Grupo emitiría una carta dirigida a la ICANN subrayando los puntos de la «Posición Común sobre Intimidad y Aspectos de Protección de Datos relativos al Registro de Nombres de Dominio en Internet», elaborada por el Grupo en la reunión de mayo de 2000 celebrada en Creta.

Asimismo, se presentaron dos documentos sobre Sistemas de Detección de Intrusiones (IDS), que fueron discutidos con interés. Estos sistemas permiten la identificación de usos no autorizados en las redes y Sistemas Informáticos, ayudando a su prevención y a la lucha contra los «piratas informáticos» o *hackers* que llegan a utilizar para sus actividades programas informáticos disponibles gratuitamente en Internet. Los representantes franceses comentaron como ejemplo un caso acaecido en su país, donde una asociación, durante la realización de pruebas de seguridad sobre los Sistemas de Información de una empresa, había conseguido extraer una base de datos de los clientes de la entidad incluyendo los nombres de los mismos y sus números de tarjetas de crédito. Finalmente, se decidió elaborar un documento de trabajo sobre aspectos de Protección de Datos y Sistemas IDS, que sería discutido en la siguiente reunión del Grupo.

Se trataron las implicaciones de Protección de Datos del nuevo protocolo denominado ENUM, definido por el IETF *(Internet Engineering Task Force)*. Este protocolo de comunicaciones, trata de integrar el mundo de la telefonía con el mundo Internet, creando nombres de dominio a partir de los números de teléfono tal y como los conocemos (Recomendación E.164 de la ITU[19]). A cada nombre de dominio así creado, se le pueden asociar una lista de servicios de comunicaciones, como pueden ser Telefonía sobre IP, fax, correo electrónico y páginas *web* , entre otros, de tal forma que a partir de un número de teléfono, se podrán alcanzar usuarios utilizando estos otros diferentes métodos. Es decir, conocido el número de teléfono del destinatario, podrá, por ejemplo, ser enviado un correo electrónico al mismo, sin necesidad conocer su dirección de correo. Si bien el Grupo reconoció la necesidad del seguimiento de este tipo de desarrollos, la elaboración de un documento de trabajo en relación con los mismos es pospuesta a posteriores reu-

niones del Grupo, a la espera de la implantación de proyectos pilotos y de la consolidación de esta tecnología.

Se habló también de la tributación de actividades realizadas por Internet. La preocupación se plantea porque los intentos de someter a tributación las actividades que se desarrollan a través de Internet conllevarán el fin del anonimato en la red, toda vez que puede suponer la creación de ficheros de personas asociados a direcciones de correo electrónico en poder de la Administración Tributaria.

Otra cuestión controvertida que se discutió fue la publicación de datos personales a través de Internet, concretamente de las consecuencias que la publicación de sentencias judiciales, cuando estas contienen los datos identificadores de los sujetos implicados. No obstante el problema se complica en los sistemas legales anglosajones que utilizan constantemente los precedentes judiciales que, por tradición, se identifican por el apellido de los litigantes. Además, con independencia de que de ahora en adelante los responsables de las bases de datos jurídicas adopten estas cautelas de anonimizar las resoluciones judiciales, se planteó el problema con las bases jurídicas ya existentes con datos personales y la dificultad de exigir la supresión de todos estos datos identificadores en ellas.

Sobre el problema del *spam*, esto es, las comunicaciones electrónicas comerciales no solicitadas, la CNIL informó sobre la actividad que están realizando mediante un buzón abierto a tal efecto, y donde los ciudadanos pueden remitir los mensajes no solicitados que reciben directamente desde su ordenador personal[20].

Para finalizar, se expusieron los riesgos que puede suponer la videovigilancia en sitios públicos y, en conjunto en medios de transporte como el Metro, poniéndose de manifiesto la necesidad de que existan las garantías adecuadas como, por ejemplo que la instalación de las cámaras debe ser exclusivamente por motivos de seguridad, que las cámaras no deberán estar dirigidas sobre una única persona (por ejemplo en el lugar de trabajo), que las imágenes grabadas sólo deberán ser almacenadas durante el tiempo mínimo necesario en relación con la finalidad perseguida. Y la necesidad de informar de la grabación de imágenes mediante carteles indicativos colocados en los lugares de donde se sitúen las cámaras.

---

[19] Unión Internacional de Telecomunicaciones

[20] Este importante estudio y las conclusiones correspondientes pueden ser consultadas en la página web de la propia CNIL (http://www.cnil.fr/thematic/index.htm).

8. Conferencia Europea de Autoridades de Protección de Datos (Bonn, 25 – 26 de abril de 2002)

La Conferencia anual de Autoridades Europeas de Protección de datos se celebró el año 2002 en la ciudad alemana de Bonn, siendo organizada por la oficina del Comisionado Federal de Protección de Datos. A pesar de que todas las autoridades de control europeas mantienen unos continuos lazos de colaboración –y de manera muy especial las de los Estados miembros del Espacio Económico Europeo (UE, Noruega, Islandia y Liechtenstein) y de los países candidatos a ingresar en la UE a través de su pertenencia al Grupo de Trabajo del Artículo 29, ya sea en calidad de miembros o de observadores y de otras Autoridades Comunes de Control de III Pilar, como ya se ha expuesto anteriormente- existe el acuerdo general de la necesidad de que exista un foro distinto en el que se puedan debatir tanto temas que no encuentran cabida dentro de las funciones propias de dichos comités como la profundización o tratamiento desde un punto de vista diferente de asuntos que han formado o formarán parte en el futuro inmediato de las agendas de dichos grupos.

En la conferencia correspondiente al año 2002, los temas más relevantes que se trataron durante la misma fueron:

- Experiencias tras el 11 de septiembre de 2001: Leyes de seguridad y el derecho de los ciudadanos a la protección de datos. La situación en Europol. La situación en el ámbito nacional.

- Auditoría / Certificación de estrategias para una mejor protección de datos y una mayor seguridad de los mismos.

- Procedimientos de identificación biométrica.

- Informes sobre la situación en los países de Europa Central y Oriental y las últimas reuniones de los Grupos de Trabajo sobre ficheros policiales y tramitación de reclamaciones.

- Diversos aspectos de la Administración electrónica.

- El proyecto de la Academia Europea para la Libertad de Información y la Protección de Datos.

- Control y verificación del último censo de población y viviendas en España. Esta presentación corrió a cargo del Director de la APD.

- Cuestiones de la transposición de la aplicación de la Directiva 95/46/CE frente a terceros países.

9. Encuentro de Representantes de las Autoridades de Control Europeas Relativo al Tratamiento y Tramitación de Reclamaciones

En el transcurso del pasado año 2002, 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 Dublín –marzo de 2002- y en Berlín –noviembre de 2002-. 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 Europea. Así mismo, se invitó por primera vez al quinto encuentro, celebrado en Berlín, del Grupo a diez países candidatos a formar parte de la Unión Europea: República Checa, Polonia, Hungría, Eslovaquia, Eslovenia, Letonia, Estonia, Lituania, Chipre y Malta.

El objetivo primordial de los encuentros del Grupo 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»

(Communication and Information Resource Centre Administrator) —página *web* creada para el intercambio de información sobre casos relativos a reclamaciones internacionales o denuncias en las que se encuentran involucradas dos o más Autoridades de Control—.

Así mismo, otros temas que han ocupado la actividad del Grupo en las reuniones mantenidas hasta el momento:

- Análisis y explicación detallada del contenido de las diferentes páginas *web* de las distintas Autoridades de Control así como de los distintos procedimientos en materia de tramitación de quejas.

- Presentación de la *website* por parte de los países de Europa Central y Oriental en materia de cooperación en el ámbito de la privacidad, operativa desde primavera de 2002.

- Internet y la amenaza que puede representar a la privacidad de los individuos, especialmente a los menores de edad.

- Tratamiento de datos en Internet.

- Niveles de privacidad establecidos por defecto. Estándares de privacidad en Internet.

- Oficina virtual de privacidad. Auditorías de protección de datos y sellos de calidad.

- Protección de datos en el ámbito laboral, en especial en lo relativo a la vigilancia y control de las comunicaciones electrónicas de los trabajadores.

- Recomendación de la Comisión de 7 de diciembre de 2001, en vigor desde el 1 de junio de 2002, y mediante la que se establecen los principios de utilización de la red de resolución de conflictos en el seno del Mercado Interior, denominada SOLVIT.

- Ficheros relativos a datos de salud.

- Videovigilancia.

- Protección de datos y política.

- Servicios de solvencia patrimonial y crédito.

Así mismo, en el seno del Grupo se distribuyeron, cumplimentaron y presentaron los resultados de dos cuestionarios circulados a las distintas Autoridades de Control relativos a

«Poderes y actuaciones de las Autoridades de Control» en materia de peticiones de información, tramitación de quejas, denuncias, inspecciones, sanciones, aplicación práctica y datos numéricos, así como un segundo cuestionario sobre «Transferencias Internacionales de datos personales», que incluye la normativa aplicable a transferencias internacionales en cada Estado miembro, el papel desempeñado por las Autoridades de Control, criterios de adecuación empleados por las Autoridades para autorizar transferencias internacionales, procedimientos y sistemas de autorización y notificación de transferencias internacionales de datos personales a terceros países.

Por último, cabe mencionar que en el marco de la cooperación multilateral y de carácter informal establecida en el marco del Grupo de Tratamiento y Tramitación de Reclamaciones, se dan curso por parte de esta Agencia a multitud de consultas y solicitudes de asesoramiento procedentes de otras Autoridades de Control referidas fundamentalmente a cuestiones de protección de datos en relación con otras materias o regulaciones de ámbito nacional.

10. Conferencia Internacional de Autoridades de Protección de Datos (Cardiff, 9 a 11 de septiembre de 2002)

La cita anual de las Autoridades de Control de Protección de Datos existentes en todo el mundo se celebró el año 2002 en Cardiff (Reino Unido), siendo los anfitriones de la conferencia las autoridades de control del Reino Unido, República de Irlanda, Isla de Man, Jersey y Guernsey que la organizaron de forma conjunta. Durante el transcurso de la misma se pasó revista a los principales desarrollos tecnológicos con influencia en la protección de datos personales que se habían sucedido en el último año y se analizaron las distintas opciones existentes para proporcionar una efectiva implantación de los principios de protección de datos en la sociedad.

Así, los temas más relevantes tratados en la conferencia fueron:

- Los principios de protección de datos, al impedir el uso compartido de la información, obstaculizan tanto la modernización de la Administración como la eficiencia en los negocios - ¿mito o realidad?

- ¿Puede la tecnología jugar un papel importante como protector de la privacidad cuando se comparte información?

- Uso compartido de la información - ¿la clave para la Administración electrónica?

- El crecimiento de la utilización de la información crediticia - ¿amenaza para la protección de datos o necesidad económica?

- El anonimato no tiene cabida en la era de los sistemas globales de información y el terrorismo internacional - ¿mito o realidad?

- El uso de la tecnología para satisfacer la demanda de identificación segura - ¿amenaza para la privacidad o instrumento para incrementarla?

- Entendiendo los negocios electrónicos - ¿podemos permanecer anónimos en el mercado global?

- ¿Son las tarjetas inteligentes la respuesta a los problemas de identificación y autenticación?

- La protección de datos personales sólo puede conseguirse a través de la existencia de autoridades de protección de datos independientes y poderosas - ¿mito o realidad?

- Autorregulación efectiva - ¿protección genuina o contradicción en los términos?

- Protección de datos, libertad de expresión y libertad de información - ¿principios contradictorios o derechos complementarios?

- La autoridad de protección de datos - ¿regulador, *ombudsman*, educador o activista?

La delegación española participó activamente en todos los trabajos de la conferencia y el Director de la APD realizó una presentación sobre como la misma lleva a cabo en la práctica todas las competencias que la LOPD y el EAPD le atribuyen.

Asimismo, se celebraron varias sesiones a puerta cerrada exclusivamente reservadas a las autoridades de control, incluyendo una general y dos paralelas que agrupaban a las autoridades europeas, por un lado, y a las no-europeas por otro.

En concreto, las autoridades europeas aprobaron una Resolución sobre la retención de datos de tráfico que, por su interés, se transcribe a continuación:

DECLARACIÓN DE LAS AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS EN LA CONFERENCIA INTERNACIONAL CELEBRADA EN CARDIFF (9-11 DE SEPTIEMBRE DE 2002) SOBRE LA RETENCIÓN SISTEMÁTICA OBLIGATORIA DE DATOS SOBRE TRÁFICO DE TELECOMUNICACIONES

«Las Autoridades Europeas responsables de la protección de datos han observado con inquietud que, en el marco del tercer pilar de la UE, se consideran propuestas que podrían implicar

la retención sistemática obligatoria de datos de tráfico referentes a todo tipo de telecomunicaciones (es decir, detalles sobre el tiempo, el lugar y los números utilizados por teléfono, fax, correo electrónico y otros usos de Internet) durante un período de un año o más, para permitir el posible acceso por los organismos de aplicación de la ley y de seguridad.

Las Autoridades Europeas responsables de la protección de datos tienen serias dudas respecto a la legitimidad y legalidad de unas medidas tan amplias. También quieren llamar la atención sobre el coste excesivo que supondrían las medidas para el sector de las telecomunicaciones y para Internet, así como sobre la ausencia de tales medidas en los Estados Unidos.

Las Autoridades Europeas responsables de la protección de datos han puesto de relieve en varias ocasiones que tal retención sería una invasión incorrecta de los derechos fundamentales garantizados a los individuos por el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, elaborado por el Tribunal Europeo de Derechos Humanos (véase el Dictamen 4/2001 del Grupo de Trabajo del artículo 29 establecido en virtud de la Directiva 95/46/CE, y la Declaración de Estocolmo, de abril de 2000).

La protección de datos sobre tráfico de telecomunicaciones ahora también está prevista ahora por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas (Diario Oficial L 201/37), en virtud de la cual el tratamiento de datos de tráfico está permitido, en principio, para facturación y para pagos de interconexión. Tras debates prolongados y explícitos, la retención de datos de tráfico con vistas a la aplicación de ley debería respetar estrictas condiciones de conformidad con el apartado 1 del artículo 15 de la Directiva: es decir, en cada caso sólo por un período limitado y cuando constituya una medida necesaria proporcionada y apropiada en una sociedad democrática.

Por lo tanto, cuando en casos específicos se deban retener datos de tráfico, debe haber una necesidad demostrable, el período de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la ley, de manera que proporcione suficientes salvaguardias frente a un acceso ilegal o cualquier otro abuso. Una retención sistemática de todas las clases de datos de tráfico para un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso.

Las Autoridades Europeas responsables de la protección de datos esperan que se consulte al Grupo de Trabajo del artículo 29 sobre las medidas que pueden surgir de las negociaciones del tercer pilar antes de que se adopten.»

11. III Encuentro Ibérico de Protección de Datos

Desde el año 2000, en el que se celebró en la ciudad portuguesa de Évora el Primer Encuentro Ibérico de Autoridades de Control de Protección de Datos, la Agencia española de Protección de Datos y la Comisión Nacional de Protección de Datos portuguesa se vienen reuniendo durante dos días de intenso trabajo una vez al año para analizar y pasar revista a los temas relativos a la protección de datos personales que más influencia tienen en la actividad de ambas para fomentar un mutuo conocimiento de las posturas e interpretaciones que cada una de ellas lleva a cabo y, en la medida de lo posible, armonizar sus actuaciones ya que la creciente relación política, económica y social entre ambos países lleva aparejada la existencia de problemas comunes a los que conviene acercarse desde una perspectiva coordinada.

De esta manera, en el año 2002 se celebró, en Arrábida (Portugal) el III Encuentro Ibérico los días 12 y 13 de noviembre. En el mismo, siguiendo el esquema habitual de las pasadas ediciones, se presentaron, a través de ponentes de cada delegación, los puntos de vista de cada una de las autoridades en los temas elegidos para, posteriormente, poner en común los problemas y debatir la mejor forma de aproximarse a soluciones comunes en cada campo.

Los temas que se debatieron con mayor profundidad fueron los tratamientos de datos personales en las oficinas de farmacia, los tratamientos de datos biométricos, el análisis de la nueva Directiva 2002/58/CE relativa a la privacidad en las comunicaciones electrónicas y los problemas derivados de la creciente utilización de los sistemas de videovigilancia.

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.

Por su interés, a continuación se incluyen las conclusiones del Encuentro.

III ENCUENTRO IBÉRICO DE
AUTORIDADES DE PROTECCIÓN DE DATOS

Arrábida, 12 y 13 de noviembre de 2002

«La Comisión Nacional de Protección de Datos (CNPD) y la Agencia de Protección de Datos (APD) se reunieron en el III Encuentro Ibérico de Autoridades de Protección de Datos, los días 12 y 13 de noviembre de 2002, en el Convento de Arrábida, en Portugal.

En este Encuentro se debatieron los «Tratamientos de datos personales en las oficinas de farmacia», los «Datos Biométricos», la «Videovigilancia» y la «Nueva Directiva de privacidad en las comunicaciones electrónicas (Directiva 2002/58//CE)».

Estas materias eran de interés mutuo para las dos autoridades tanto por la posibilidad de intercambiar experiencias de métodos de trabajo, soluciones adoptadas y las respectivas especificidades legislativas como por la posibilidad de abordar y debatir asunto que han dado lugar a nuevas cuestiones sobre la protección de datos personales. La rápida implantación de nuevas tecnologías y la generalización de su uso masivo suponen un verdadero desafío para las Autoridades de Protección de datos en la medida en que su noviedad y complejidad exigen un profundo estudio y una mayor ponderación de los intereses en presencia, al mismo tiempo que resulta necesario intervenir de inmediato en la defensa de la privacidad de los ciudadanos.

En relación con el tratamiento de datos personales por parte de las oficinas de farmacia, se comparó el funcionamiento de los sistemas de información utilizados. A pesar de que el régimen jurídico subyacente a estos tratamientos es muy diferente en ambos países, la perspectiva de las dos autoridades, ya expresada en distintas resoluciones, es semejante en cuanto al nivel de protección que debe asegurarse al tratamiento de estos datos, dado que están incluidos datos sensibles, especialmente en lo que se refiere a las medidas organizativas y de seguridad y de la garantía del derecho de información a los afectados.

En lo que respecta al tratamiento de datos biométricos, se verificó que se han notificada muy pocos casos concretos a las Autoridades. No obstante, existió un consenso entre ambas delegaciones en el sentido de que existe una aplicación creciente de este tipo de sistemas y que las Autoridades de Protección de Datos necesitan estar preparadas para responder a esta nueva realidad, que no se encuentra reglamentada por ningún tipo de legislación específica.

Partiendo del principio, unánimemente aceptado, de que los datos biométricos son datos personales, la discusión se centró en la calificación de la naturaleza de estos datos.

Dadas las características especiales que revisten a los datos biométricos, los principios de finalidad y de proporcionalidad en el tratamieno de estos datos adquieren una importancia fundamental, en el sentido de asegurar que no sean utilizados indebidamente.

En cuanto al análisis de la nueva Directiva sobre privacidad en las comunicaciones electróncias, se concluyó que, introduciendo nuevos conceptos y extendiendo su objeto, se solucionaban multitud de problemas y lagunas existentes que daban a las Autoridades muchos problemas concretos de protección de datos en este sector. No obstante, se constató que existen dificultades de transposición de algunas garantías debido a las diferencias de contendio entre algunos Considerandos y los respectivos artículos. Esta circunstancia permite distintas interpretaciones a los Estados miembros, corriéndose, pues, un serio riesgo de que resulten transposiciones al Derecho internos muy diferentes, lo que será claramente perjudicial en materias de naturaleza especialmente transfronteriza.

Las Autoridades de Protección de Datos ibéricas consideraron útil recordar a los respectivos Estados que el plazo de transposición termina el 31 de octubre de 2003. Con este propósito, se decidió informarse mutuamente de los dictámentes que ambas autoridades elaboraran.

En relación con la videovigilancia, ambas Autoridades constataron el creciente uso de estas técnicas, sobre todo en el ámbito de la seguridad pública y privada. Se analizó el marco jurídico de los dos países y las dificultades para determinar los principios de protección de datos legitimadores de dichos tratamientos, dada la gran diversidad de finalidades y tecnologías utilizadas. Ambas delegaciones consideraron que sería útil contar con una regulación específica, en los dominios donde no exista, que contemple las utilizaciones posibles y las garantías que permitan encontrar un equilibrio que respete los derechos de los ciudadanos.

Las dos Autoridades reiteran el interés común de mantener este tipo de Encuentro para estrechar las relaciones bilaterales e intercambiar ideas y experiencias.»

12. Conferencia Sobre los Retos a los que Deben Enfrentarse las Autoridades de Control Recientemente Establecidas (Conferencia de Madrid)

La Agencia de Protección de Datos y el Consejo de Europa organizaron conjuntamente en el mes de diciembre de 2002, una Conferencia sobre los retos a los que deben enfrentarse las autoridades de control recientemente establecidas, dirigida fundamentalmente a aquellos países de Europa Central y Oriental que han aprobado recientemente leyes de protección de datos y están estableciendo autoridades de control independientes para supervisar su cumplimiento.

La Conferencia fue inaugurada por el Excmo. Sr. Ministro de Justicia, D. José María Michavila Núñez y en la misma, además de representantes de España y del Consejo de Europa, participaron delegados de Azerbaiján, Bulgaria, Bosnia-Herzegovina, Canadá, Croacia, Chipre, Estonia, Francia, Georgia, Hungría, Italia, Letonia, Lituania, Malta, Moldavia, Portugal, Rumanía, República Checa, República Eslovaca, Países Bajos, Polonia, República de Macedonia, República Federal de Yugoslavia (hoy Serbia y Montenegro), Rusia, Suiza y Ucrania, así como representantes de la Comisión Europea y la Organización para la Cooperación y el Desarrollo Económico (OCDE).

La Conferencia se estructuró en torno a aquellos temas que resultaban de mayor interés para las autoridades de reciente creación. Para la preparación de los mismos, se encargó a distintos relatores la elaboración de un informe preparatorio así como la elaboración de conclusiones finales por cada uno de los puntos.

En concreto, se celebraron sesiones relativas a los siguientes temas:

- Características principales de las autoridades de protección de datos y procedimiento para su puesta en funcionamiento. Protocolo Adicional al Convenio 108 del Consejo de Europa

- Mecanismos para la puesta en funcionamiento de los principios de la protección de datos establecidos en el Convenio 108 del Consejo de Europa

- Las relaciones entre las autoridades de control de protección de datos y los responsables de los datos

- Los desafíos producidos por los flujos transfronterizos de datos de carácter personal

- Contribución de las autoridades de control subestatales para la eficaz implantación de los principios de protección de datos

Además, el Director de la APD, en su conferencia inaugural trató el tema de *«La experiencia de intercambio de información entre la Agencia de Protección de Datos de España y las nuevas autoridades de control de protección de datos»*.

Esta conferencia tuvo como marco de referencia la reciente apertura a la firma de los Estados miembros del Consejo de Europa del Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, que establece nuevos requisitos de independencia y poderes de supervisión efectivos para las autoridades de supervisión en materia de protección de datos, así como la restricción a las transferencias de datos personales a aquellos países no Partes del Convenio 108 que no garanticen un nivel de protección adecuado.

Tras las distintas intervenciones que ponían de manifiesto la situación de las nuevas autoridades así como la experiencia de otras más veteranas en la resolución de los distintos problemas, se mantuvieron interesantes debates que contribuyeron a un mejor entendimiento de los distintos asuntos así como al mutuo conocimiento de las autoridades participantes[21].

[21] Las actas de la Conferencia pueden consultarse en http://www.coe.int/dataprotection/ bajo el epígrafe «Events».

13. Otras Actividades de Ámbito Internacional

13.1. Conferencia sobre la transposición de la Directiva 95/46/CE

La Directiva 95/46/CE establece en su artículo 33 que la Comisión Europea debe presentar informes periódicos al Consejo y al Parlamento Europeo sobre la aplicación de la misma, realizando, en su caso, las oportunas propuestas de modificación. El primero de estos informes debería haberse presentado en un plazo de tres años a partir del mes de octubre de 1998, pero diversos factores, incluyendo el retraso con que una buena parte de los Estados miembros transpusieron la Directiva (proceso que aun a día de hoy no está finalizado), han motivado que el mismo no vaya a estar disponible hasta el año 2003.

Con objeto de obtener información al respecto, la Comisión Europea ha utilizado distintas vías, incluyendo la remisión de cuestionarios muy detallados a las autoridades de control y a los gobiernos de los Estados miembros, el encargo a un experto externo de un informe jurídico sobre la materia, el lanzamiento a través de Internet de una consulta *on-line* a los ciudadanos y responsables de tratamientos sobre su percepción del nivel de protección existente en Europa y la identificación de sus puntos más débiles y la petición a las organizaciones empresariales y de consumidores de su opinión al respecto.

No obstante, antes de emitir su informe definitivo, la Comisión quiso culminar todo el proceso de recogida de información con la celebración en Bruselas, durante los días 30 de septiembre y 1 de octubre de 2002, de una «Conferencia sobre la transposición de la Directiva 95/46/CE», en la que pudieran participar todos los actores interesados en la protección de datos personales en Europa y que le permitiera escuchar de primera mano las distintas posiciones y propuestas que cada uno de ellos formulara en el curso de los debates[22].

Los trabajos de la misma se estructuraron en torno a seis sesiones de trabajo que giraron en torno a como mejorar la transposición de la Directiva; los desarrollos en las Tecnologías de la Información: Internet y las Tecnologías de Mejora de la Privacidad (PETs); el tratamiento de datos personales de sonido e imagen; temas de ámbito internacional como las transferencias internacionales y la ley y jurisdicción aplicable a los tratamientos transnacionales; derechos e intereses de los afectados y, finalmente, sobre las distintas posibilidades existentes para mejorar el cumplimiento de la legislación de protección de datos, incluyendo la educación, la supervisión y la autorregulación.

La APD fue invitada a presentar contribuciones en dos de las sesiones más importantes: la dedicada a los aspectos internacionales y participando (que fue presidida por su Director) y aquella en la que se estudiaron los mecanismos para un mejor cumplimiento de la ley.

Como conclusiones de la Conferencia, podemos resaltar las mencionadas por el Comisario Frits Bolkestein en su discurso de clausura, en el que resaltó que, en su opinión, la Directiva había cumplido sus objetivos principales: la libre circulación de datos personales es una realidad en la Unión y todos los países se han dotado de una legislación que garantiza un alto nivel de protección a sus ciudadanos.

No obstante, también indicaba que, a la vista de toda la información recibida por la Comisión, el Informe final haría referencia a una serie de puntos en los que existía un cierto margen para mejorar:

- la simplificación de los procedimientos de notificación
- reducción de las divergencias, para lo cual se esperaba que el Grupo de Trabajo del Artículo 29 juegue un papel capital incrementando, además, la transparencia de sus métodos de trabajo
- promoción de las Tecnologías de Mejora de la Privacidad (PETs)
- soluciones más flexibles para las transferencias internacionales de datos y una mayor uniformidad en la interpretación de las reglas

[22] Tanto el programa como las contribuciones de los ponentes en esta Conferencia pueden consultarse en http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm

- promoción de la autorregulación a través de los Códigos de Conducta, no descartando la posibilidad de que, en el futuro, exista algún mecanismo de reconocimiento mutuo que permita que un código aprobado por una autoridad de control de un Estado miembro implique la validez en toda la UE

13.2. Países de Europa Central y Oriental

Como ya se ha puesto de manifiesto en anteriores ediciones de esta Memoria, 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 APD no puede desconocer este hecho y 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 UE en este campo se lleve a cabo en las mejores condiciones posibles.

13.2.1. Actividades generales

En primer lugar, pasaremos revista a toda una serie de actividades bilaterales con diversos países de Europa Central y Oriental, para describir con más detalle en el apartado siguiente, el Proyecto de Hermanamiento con la República Checa que, por su especial significación, merece comentario aparte.

Durante el año 2002 han continuado las estrechas relaciones de trabajo con la Inspección General polaca, que es como se denomina la autoridad de control de protección de datos en ese país, estando previsto para el año 2003 la realización de una nueva visita de trabajo de una delegación de la Agencia a este país para comprobar la evolución de la situación desde la anterior visita que se produjo en el año 2000.

Asimismo, un representante de la APD participó como experto en otro Proyecto de Hermanamiento de los Ministerios del Interior de España y la República Eslovaca.

A tal efecto, impartió un seminario a representantes de los distintos cuerpos de policía eslovacos así como a las personas encargadas de la supervisión del cumplimiento de las reglas de protección de datos por estos organismos. El seminario tuvo como tema monográfico el estudio de los aspectos más relevantes de protección de datos personales que deberán implantarse en los ficheros de las fuerzas y cuerpos de seguridad eslovacos para

adaptarse a las exigencias derivadas de su participación en los Convenios de Schengen, Europol y Sistema de Información Aduanero y a cómo estas obligaciones han sido implantadas en España. Finalmente, se pasó revista a todos los aspectos relevantes de protección de datos personales presentes en los convenios antes mencionados.

Con dicho objeto, durante el desarrollo del seminario se abordaron temas relativos a los principios esenciales del Convenio 108 del Consejo de Europa; los principios y de la Recomendación (87) 15, también del Consejo de Europa sobre tratamientos de datos personales en el sector de la policía; al examen de la incorporación al Derecho español de ambas normas haciendo especial hincapié en la regulación contenida en la Ley Orgánica 15/19999, de 13 de diciembre, de protección de datos de carácter personal y en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad y a la presentación comparativa de los aspectos de protección de datos de los Convenios de Schengen, Europol y Sistema de Información Aduanero, celebrados en el marco del III Pilar así como el Reglamento EURODAC.

También hay que destacar que el Director de la Agencia de Protección de Datos realizó una visita al Comisionado de Protección de Datos y Libertad de Información húngaro, durante la que se trataron temas de interés común y diversas medidas para incrementar la cooperación entre ambas autoridades.

Finalmente, para terminar el capítulo de cooperación con los países del Centro y Este de Europa, hay que referirse a la participación de la APD en las *Peer Reviews* (o Revisiones entre iguales) que, auspiciadas por la Comisión Europea, se han llevado a cabo durante el mes de junio de 2002 en las autoridades de control de Hungría y la República Checa.

En estas *Peer Reviews*, miembros de las autoridades de control de la Unión Europea debían evaluar, desde un punto de vista eminentemente práctico, el efectivo cumplimiento por parte de dichas autoridades de los requisitos que la legislación comunitaria establece para una autoridad de control de este tipo.

Así, un experto de la APD fue miembro de los equipos multinacionales (compuestos, además, por representantes de Bélgica y el Reino Unido en Hungría y Portugal y Alemania en el caso checo) que llevaron a cabo estas auditorías cuyo objetivo final era la emisión de un informe para la Comisión Europea en el que se pusieran de manifiesto la situación real de dichas autoridades en el momento de la realización de la revisión.

Hay que hacer notar que los equipos de auditoría estaban formados por personas con amplia experiencia en las labores propias de una autoridad de control por lo que las revisiones fueron exhaustivas y en ambos casos con resultados francamente satisfactorios, no sólo para las autoridades auditadas, sino también para los auditores que tuvieron la opor-

tunidad de intercambiar ideas y puntos de vista con los excelentes profesionales que desempeñan su labor en estas autoridades.

13.2.2. República Checa

Por ello, la APD viene colaborando de forma continuada con distintos países de esa área geográfica, revistiendo, hasta el momento presente, una especial importancia las relaciones con la Oficina de Protección de Datos de 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 Proyecto de hermanamiento es resultado del Convenio firmado entre las instituciones hermanadas y ratificado por la Comisión Europea en fecha 26 de julio de 2001.

Tal y como se indica en el Convenio, su propósito es *«apoyar el pleno establecimiento al final de 2002 de la Oficina para la Protección de Datos de Carácter Personal- creada por la Ley No. 101/2000- con el desarrollo de sistemas adecuados de control y administración, el establecimiento de su capacidad técnica y el personal debidamente formado, a fin de garantizar una regulación de protección de datos efectiva, no discriminatoria y transparente, de acuerdo con el acervo comunitario».*

Las actividades desarrolladas durante el Proyecto fueron las siguientes:

Actividades relacionadas con el análisis de marco legislativo:

Dentro de este apartado cabe distinguir, las actividades relacionadas con la normativa general de protección de datos y con las normas sectoriales que afectan a esta materia.

En cuanto al marco general, se han realizado las actividades tendentes al pleno cumplimiento de la Directiva 95/46/CE por parte de la Ley checa de Protección de datos. Del mismo modo, se han elaborado propuesta de desarrollo de las previsiones contenidas en la Ley checa de protección de datos. En este sentido cabe hacer referencia a los siguientes documentos:

- Informe sobre la adecuación de la Ley checa de Protección de Datos a la Directiva 95/46/CE, incluyendo las correspondientes propuestas normativas.

- Informe sobre propuestas de desarrollo de la Ley checa de protección de datos en lo referente a la seguridad en el tratamiento de los datos.
- Normas referentes a los procedimientos de notificación, autorización de transferencias internacionales y tramitación de procedimientos de inspección e imposición de sanciones, contenidas en los manuales referentes a estas áreas de actividad.

En cuanto al estudio de la normativa sectorial en materia de protección de datos, se han elaborado distintos documentos analizando las normas actualmente vigentes en la materia en la República Checa e incorporando las conclusiones y propuestas legislativas que se han considerado necesarias. Así, cabe hacer referencia a los informes relacionados con las siguientes áreas:

- Legislación bancaria y relativa a los sistemas de información de crédito.
- Telecomunicaciones.
- Firma electrónica.
- Comercio electrónico.
- Tratamiento de datos por la policía.
- Tratamiento de datos en el sector sanitario.

Al propio tiempo, se han mantenido estrechos contactos de colaboración con las autoridades de la Unión Europea a fin de poder dar debida explicación de la problemática del ordenamiento jurídico checo en su conjunto y permitir la realización de actuaciones conjuntas tendentes a mejorar ese marco normativo.

Actividades relacionadas con el análisis de la estructura y recursos humanos de la Oficina Checa:

Se ha procedido al análisis de la situación existente en la Oficina Checa y de la adecuación del personal contratado a sus actividades, tomando como punto de referencia la situación que se da en otras autoridades de protección de datos de los Estados Miembros de la Unión Europea. En dicho estudio se indica también cuál es la estructura ideal de una autoridad de protección de datos y el personal mínimo con el que la misma debe contar, poniéndose de manifiesto la situación de la Oficina checa y adoptando las conclusiones pertinentes.

Actividades relacionadas con la formación:

A lo largo de la vigencia del Proyecto se han realizado diversas actividades dentro del marco al que nos estamos refiriendo:

- Dos seminarios generales sobre protección de datos, que tuvieron lugar en Praga, en febrero y junio de 2002.
- Reunión de trabajo con el Departamento de inspección en Praga en marzo de 2002.
- Reunión de trabajo sobre tramitación de procedimientos, celebrada en Praga en marzo de 2002.
- Dos visitas de estudio de representantes del Departamento de Inspección, referidas tanto al análisis de supuestos concretos de inspección material realizados en España como al estudio de los distintos procedimientos tramitados para la resolución de las quejas planteadas por los ciudadanos o la imposición de sanciones a los responsables y encargados de los tratamientos. Estas visitas se realizaron en mayo y julio de 2002, participando en las mismas diez miembros del personal de la Oficina checa.
- Visita de estudio para el análisis del sistema de notificación de tratamientos establecido por la Agencia española y sus diferencias con el sistema de la Oficina checa, celebrada en diciembre de 2001 con participación de 4 expertos checos.
- Reunión de trabajo en Praga, complementaria de la anterior, en mayo de 2002.
- Reunión de trabajo sobre actividades internacionales de las autoridades de protección de datos y tramitación de expedientes de autorización de transferencias internacionales de datos, celebrada en abril de 2002 en Praga.

Actividades relacionadas con la regulación del funcionamiento interno y seguimiento de las actividades:

Estas actividades se refieren en especial a los cuatro ámbitos fundamentales de actividad de la Oficina checa, nos referiremos a ellos separadamente.

Así, en primer lugar, en cuanto a la actividad de notificación y registro de los tratamientos, las actividades se han centrado en dos actividades esenciales:

- La elaboración de un manual de tramitación de los procedimientos de notificación de los tratamientos a la autoridad de protección de datos, teniendo en cuenta las reglas que han de seguirse para proceder o no al registro de dichos tratamientos.
- La realización de un estudio específico sobre el Departamento del Registro y el procedimiento de notificación, proponiendo las medidas que se han considerado oportunas.

En segundo lugar, en cuanto a la actividad de inspección, cabe también hacer referencia a las siguientes actividades esenciales:

- La preparación de un manual de inspección.

- La realización de un plan de inspección, centrado en el sector sanitario, con participación de dos expertos de la APD, que han mantenido reuniones de trabajo con los inspectores checos en junio y septiembre de 2002.
- La realización de un informe general sobre los planes de inspección, con la propuesta de los sectores que deberían ser objeto de inspección en el período 2002-2005.

En cuanto a la tramitación de procedimientos, las actividades son:

- Elaboración de un manual sobre procedimientos, con especial estudio del procedimiento sancionador.
- Seguimiento y colaboración del Consejero Pre Adhesión con el personal de la Oficina en los supuestos en que ha resultado necesaria.

Por último, en lo referente a las relaciones exteriores y, en especial, con las Instituciones de la Unión Europea, cabe destacar:

- La elaboración de un manual sobre procedimientos de autorización de transferencias internacionales de datos, con especial análisis de los distintos supuestos en que cabe considerar, desde el punto de vista sustantivo, la validez de la transferencia y el estudio de los Estados que ofrecen un nivel de protección adecuado, en los términos previstos en la Directiva 95/46/CE y la Ley checa.
- Participación del Consejero Pre Adhesión, junto con el propio *Project Leader* checo, en calidad de observadores, en las reuniones del Grupo de Trabajo del artículo 29 de la Directiva que han tenido lugar en febrero y mayo de 2002 en Bruselas.
- Colaboración con las autoridades de la Oficina checa en las reuniones mantenidas con representantes de la Unión Europea para la elaboración de las propuestas de modificación de la Ley checa de protección de datos.
- Colaboración con las autoridades checas durante la *Peer Review* llevada a cabo durante el mes de junio de 2002, con participación de representantes de la Comisión Europea y tres autoridades de control de los Estados Miembros (Alemania, España y Portugal), con el fin de analizar si la autoridad checa cumple los requerimientos de la Directiva de protección de datos.

Actividades relacionadas con la colaboración en el desarrollo del sistema de información de la Oficina checa:

En desarrollo de este apartado del Convenio se han realizado las siguientes actividades:

- Visita de estudio de tres representantes de la Oficina checa a la Agencia española, para analizar con todo detalle el funcionamiento de su sistema de información, durante el mes de abril de 2002.

- Elaboración de un informe comparativo de ambos sistemas, con indicación de las posibles mejoras que pudieran implantarse en el sistema de información de la Oficina checa.

Actividades relacionadas con la divulgación de la protección de datos personales:

A lo largo del Proyecto expertos españoles se desplazaron a la República Checa con el fin de participar, junto con el Consejero Pre-Adhesión, en una serie de Seminarios relacionados con distintos aspectos sectoriales de la protección de datos de carácter personal. Así, se han celebrado los siguientes seminarios:

- Dos seminarios generales sobre protección de datos.

- Diez seminarios específicos sobre protección de datos, referidos a las siguientes materias:
  - La protección de datos en las actividades de *marketing* directo (Enero de 2002).
  - Los sistemas de información de crédito (febrero de 2002).
  - Los tratamientos realizados por las entidades aseguradoras (abril de 2002).
  - El tratamiento de datos por el sector sanitario (abril de 2002).
  - Las normas sobre protección de datos en el sector de las telecomunicaciones (abril de 2002).
  - Protección de datos en Internet (abril de 2002).
  - Los tratamientos realizados por las Administraciones Públicas (mayo de 2002).
  - El tratamiento de datos por el sector bancario (junio de 2002).
  - El tratamiento de datos genéticos (septiembre de 2002).
  - Los tratamientos efectuados por la policía. Los sistemas de información de Schengen y EUROPOL (septiembre de 2002).

Al propio tiempo, se han realizado las actividades tendentes a la adopción de medios de divulgación adicionales a los ya puestos en marcha por la Oficina.

RESUMEN GENERAL (CIFRAS):

Documentos realizados:	19
Visitas de estudio:	5
Reuniones de trabajo:	4
Seminarios:	12
Expertos checos en visitas de estudio:	23
Visitas de expertos españoles a corto plazo:	33

13.3. Iberoamérica. Encuentro de El Escorial

El acontecimiento más relevante para las relaciones de la APD con distintas instituciones de Iberoamérica con responsabilidad en el ámbito de protección de datos fue la celebración en España, los días 20 y 21 de mayo, del I Encuentro Iberoamericano de Protección de Datos, que reunión en San Lorenzo de El Escorial (Madrid) a cerca de cuatrocientos participantes y en el que presentaron contribuciones representantes de Argentina, Brasil, Costa Rica, España, México, Paraguay, Perú, Portugal y Uruguay. Además, el encuentro contó con la participación del Sr. Philippe Reanudière, Jefe de la Unidad de Protección de Datos de la Comisión Europea y del Presidente del Grupo de Trabajo del Artículo 29, Prof. Stefano Rodotà.

En el transcurso de los días que duró el Encuentro se pasó revista a una serie de cuestiones fundamentales y de especial relevancia para los participantes de América Latina, entre los que podemos destacar la configuración de la protección de datos personales como un derecho fundamental de la UE, las implicaciones de la protección de datos para el comercio electrónico, el régimen aplicable a las transferencias internacionales de datos personales a la luz de la Directiva 95/46/CE y el estudio de algunos ficheros de datos personales que resultan más sensibles para los ciudadanos (ficheros de morosos, seguros, etc.).

Pero, sin duda, uno de los aspectos más interesantes fueron las intervenciones de los representantes de los países americanos explicando la situación actual en sus respectivos países y los proyectos de futuro, tanto desde el punto de vista jurídico como tecnológico, que se estaban desarrollando en aquel momento.

Como conclusión a los dos días de intenso trabajo, los representantes latinoamericanos que asistieron al Encuentro suscribieron, junto con la APD una Declaración que, por su interés, se reproduce a continuación. No obstante, merece la pena destacarse la creación de un Secretariado permanente que, en principio, será desempeñado por la APD, para canalizar los flujos de información entre los participantes y promover la cooperación en todos los ámbitos relacionados con la protección de datos a ambos lados del Atlántico.

I ENCUENTRO IBEROAMERICANO
DE PROTECCIÓN DE DATOS
DECLARACIÓN

«Los participantes en el Encuentro Iberoamericano de Protección de Datos, convocado por la Agencia de Protección de Datos española, provenientes de Argentina, Brasil, Costa Rica, España, México, Paraguay, Perú y Uruguay, celebrado en San Lorenzo de El Escorial (España), durante los días 20 y 21 de mayo de 2002.

- *Manifiestan que el respeto a la intimidad y a la privacidad y, en particular, a libre disposición de sus datos personales, es un derecho fundamental de las personas*
- *Valoran los grandes beneficios que las nuevas tecnologías de la información y las comunicaciones y, específicamente, Internet pueden suponer para el desarrollo social y económico de los países, involucrando en estos esfuerzos a las organizaciones públicas y privadas y a los ciudadanos. Al mismo tiempo, reconocen que las personas mantienen su derecho fundamental a la libre disposición de sus datos personales independientemente de las tecnologías utilizadas en el tratamiento de los mismos*
- *Constatan la importancia y el mutuo interés de los intercambios científicos, tecnológicos, culturales y económicos entre la Unión Europea e Iberoamérica, siendo una muestra de ello la reafirmación, por parte de la II Cumbre Unión Europea-América Latina y el Caribe celebrada el pasado fin de semana en Madrid, del apoyo al proceso de negociación que mantiene la Unión Europea con el Mercosur, a la iniciación de procesos similares con la Comunidad Andina y los países centroamericanos y los recientes acuerdos de libre comercio celebrados entre la Unión Europea y algunos países de Iberoamérica*
- *Igualmente constatan que el comercio electrónico es un componente de importancia creciente en el marco de los intercambios comerciales anteriormente aludidos*
- *Asimismo, ponen de relieve que reiteradamente se ha puesto de manifiesto por distintos estudios nacionales e internacionales que la confianza de los ciudadanos en un tratamiento leal y respetuoso de sus datos personales es un factor clave para la expansión del comercio electrónico entre otros recursos proporcionados por las tecnologías digitales*
- *Que a tal efecto es importante que los países entre los cuales se producen dichas transacciones electrónicas ofrezcan un nivel de protección suficiente y que, para ello, debería promoverse una comunicación continuada entre la Unión Europea y América Latina que aborde el establecimiento de estructuras adecuadas para salvaguardar los derechos de las personas y, en particular, el derecho a la protección de datos personales.*

Para coadyuvar a la consecución de estos objetivos, los participantes en el Encuentro Iberoamericano de Protección de Datos manifiestan su intención de:

- *Promover un intercambio continuo y fluido de información respecto de la evolución de la situación en materia de protección de datos en sus respectivos países.*
- *Informar a las autoridades públicas competentes y al sector privado de sus países de las conclusiones alcanzadas en el Encuentro.*
- *Promover la adopción de aquellas medidas que pudieran favorecer la consecución de un nivel adecuado de protección de datos personales.*
- *Establecer un Foro permanente que coordine estas actuaciones, cuya Secretaría podrá ser rotatoria y que se establece en la Agencia de Protección de Datos española para los próximos dos años».*

Finalmente, como ha manifestado desde el momento de su toma de posesión el nuevo Director de la APD, el Dr. D. José Luis Piñar Mañas, la cooperación con América Latina y la contribución a la implantación en dichos países de un marco jurídico que garantice un nivel de protección de datos adecuado en los mismos, es uno de los ejes vertebradores de la acción internacional de la APD.

Otras Actividades

1. Colaboración 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 sobre protección de datos personales.

En el año 2002 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 cooperación entre ambas instituciones.

Con las Universidades se han mantenido las actuaciones dirigidas a la resolución de sus problemas como responsables de ficheros, potenciándose la participación del personal de la Agencia en la impartición de *«masters»* especializados, organizados en el seno de las mismas. Igualmente, se ha impulsado la realización de acciones formativas por parte de los alumnos universitarios en la sede de la propia Agencia, tanto en su vertiente de «prácticas», encuadradas en el «Plan de Estudios» de las facultades de Derecho, como en relación con los alumnos de postgrado, procedentes de *«masters»* organizados por la Universidad.

En concreto, durante 2002, tanto el Director de la Agencia, como el resto del personal directivo de la misma, han llevado a cabo actividades de difusión de la LOPD, participando en conferencias, seminarios y cursos especializados impartidos, entre otras Universidades, por la Complutense, la Carlos III, la de Alcalá de Henares, y la Pontificia de Comillas (ICAI-ICADE) de Madrid, y por diferentes Facultades ubicadas, entre otras ciudades, en Castellón, Oviedo, Murcia, Salamanca, Valencia, Valladolid y Zaragoza. Igualmente, fiel a esta vocación divulgativa de la LOPD, la Agencia ha mantenido una constante colaboración con Institutos y Organizaciones de Empresa, así como con Escuelas de Negocios y de Estudios Fiscales, en cuyo seno se han dictado diferentes conferencias, participando la APD en diversos Seminarios. Igualmente, el personal de la Agencia ha colaborado con diversos Grupos Editoriales, impartiendo conferencias en las sedes de «Aranzadi» y del «Grupo Recoletos».

Además, en virtud de los Convenios de Colaboración suscritos con las Facultades de Derecho de la Universidad Complutense de Madrid y de la Universidad Carlos III de Madrid, en 2002 la Agencia ha acogido en su seno, como «alumnos en prácticas», a un total de diecinueve estudiantes, a los que se ha ofrecido la oportunidad de conocer de manera general la estructura y funcionamiento de las distintas Unidades de la Agencia de Protección de Datos. Asimismo, durante el periodo de dichas prácticas, los referidos alumnos han tenido ocasión de profundizar, de manera especial, en el conocimiento de las funciones específicas de alguna de las áreas de actividad de la Agencia.

La APD ha continuado desarrollando relaciones con Corporaciones de Derecho Público y, muy especialmente, con las Cámaras Oficiales de Comercio, Industria y Navegación y los Colegios Profesionales, tomando parte en diversas Jornadas y Seminarios organizados, entre otras, por las Cámaras de Madrid, Barcelona, Vigo, La Coruña, Málaga, Cádiz, Toledo, Zaragoza, Murcia y Bilbao.

Asimismo, diverso personal directivo de la Agencia ha participado en Jornadas dirigidas específicamente a difundir el conocimiento de la Ley por profesionales y empresas, organizadas por diversos Colegios Profesionales y otros colectivos, tales como los de Farmacéuticos, Periodistas, Graduados Sociales, Gestores Administrativos, Economistas, Abogados, Titulados Mercantiles y Empresariales, Registradores, Consultores y Auditores. En 2002 se han ampliado las reuniones mantenidas con estos colectivos que presentan problemas específicos respecto de la protección de datos personales.

A los Protocolos de Colaboración firmados en años anteriores por la APD, se han unido en 2002, los suscritos con la Federación Española de Municipios y Provincias (FEMP) y con el Colegio de Registradores de la Propiedad, Mercantiles y Bienes Muebles de España. Precisamente en colaboración con la FEMP, la APD ha participado en 2002 en unas Jornadas dedicadas al estudio de la incidencia de la LOPD en el ámbito de las Entidades Locales, amén de su colaboración en Seminarios y Acciones específicas organizadas por diferentes Ayuntamientos.

En 2002 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 los Ministerios de Defensa, del Interior, de Justicia, y de Ciencia y Tecnología, así como con la Secretaría de Estado de Telecomunicaciones, el Instituto Nacional de Estadística, varias Consejerías de diferentes Comunidades Autónomas, y diversas Corporaciones Locales.

Especial mención merece la colaboración con el Ministerio de Hacienda, impulsada a través de la participación del Director de la Agencia en el VIII Encuentro de Inspectores de Hacienda de las Delegaciones Especiales de la AEAT, y la impartición de diferentes cursos sobre protección de datos personales, dirigidos al personal funcionario de Institutos Públicos y Ministerios, tales como el Instituto Nacional de Administración Pública (INAP), las Fuerzas y Cuerpos de Seguridad del Estado, el Ministerio de Sanidad y Consumo, y el Ministerio de Trabajo y Asuntos Sociales.

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. Baste aquí destacar, de manera específica, el intenso trabajo de colaboración y apoyo permanente que, durante 2002, ha mantenido la APD con la Oficina para la Protección de Datos Personales de la República Checa, en virtud del cual el personal directivo de la Agencia ha impartido diferentes conferencias y participado en diverso tipo de eventos.

También en el ámbito de sus relaciones internacionales, merecen una mención especial los contactos mantenidos por la APD con diversas embajadas y organismos extranjeros acreditados en España, al objeto de intercambiar ideas en relación con distintos aspectos referidos a la protección de datos personales, así como las diversas reuniones y conversaciones mantenidas con diferentes miembros de las Autoridades de protección de datos extranjeras y representantes de las Instituciones Comunitarias, y con diferentes autoridades gubernamentales y diplomáticas de los países que integran la Comunidad Iberoamericana de Naciones. Dentro de este ámbito, durante 2002, se ha producido un intenso intercambio de información, respondiendo la APD a las preguntas y cuestionarios remitidos por las autoridades de control de protección de datos europeas.

Asimismo, se han mantenido reuniones con representantes de empresas extranjeras radicadas en España, a fin de aclarar o explicar diversos aspectos de la legislación española y comunitaria sobre protección de datos. Fruto de esta serie de contactos, se ha conseguido una mejor comprensión de la referida normativa por parte de dichas empresas, especialmente en lo relativo al Registro de sus ficheros y a las Transferencias Internacionales de Datos.

2. Participación de la Agencia en conferencias, seminarios, jornadas y reuniones institucionales

A lo largo de 2002 han sido muy numerosos los requerimientos planteados, tanto al Director de la Agencia, como al resto del personal directivo de la misma, 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 a la APD exponer los criterios de aplicación de la LOPD contenidos en sus resoluciones así como resolver las dudas que se plantean en cada sector concreto. En este sentido, la Agencia ha mantenido constantes reuniones con diferentes responsables de ficheros privados, abordando en profundidad las peculiaridades de cada tipo de empresa.

Sin duda alguna, la Agencia de Protección de Datos es el organismo clave que la Ley Orgánica de Protección de Datos prevé para la protección de los datos personales y en consecuencia para la garantía de un derecho fundamental de enorme importancia en la sociedad actual.

Durante 2002, la Agencia ha continuado en su línea de garantía, apoyo para la correcta aplicación de la ley y prevención. A través de la participación de su personal en numerosas conferencias, seminarios, jornadas y reuniones, se ha reforzado la misión preventiva que la Agencia ha de cumplir. En este sentido, se ha puesto a la Agencia, una vez más, a disposición de cuantos quieren acercarse a ella. De este modo se ha llevado a cabo una

función preventiva en relación con la LOPD, facilitando su conocimiento y el cumplimiento de sus preceptos por parte de los operadores económicos que han de adecuar su actividad a las exigencias legales.

A su vez, a través de las diferentes acciones educativas y de difusión desplegadas durante 2002, se ha pretendido conseguir una mayor y mejor concienciación de los ciudadanos en relación con la protección de sus datos de carácter personal.

La reciente promulgación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica ha incidido muy especialmente durante 2002 en la participación del Director de la Agencia en diversos tipos de eventos, en los que se trataron las cuestiones derivadas de la aplicación de dicha norma, que entró en vigor en mayo de 2003. Asimismo, la publicación de la Ley 34/2002, de 11 julio, de servicios de la sociedad de la información y del comercio electrónico, ha fomentado la presencia de la Agencia en diferentes foros, en los que se analizó la protección de datos de carácter personal en el ámbito de las nuevas tecnologías de la información y las telecomunicaciones.

Igualmente, debe destacarse la participación de la APD en las Jornadas sobre «Régimen Jurídico de la Protección de los Datos de Carácter Personal», que tuvieron lugar en Murcia los días 29, 30 y 31 de enero de 2002, en las que se analizaron importantes aspectos relativos al derecho fundamental a la protección de datos.

Durante 2002 han continuado celebrándose 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.

A su vez, la actividad informativa del Director de la Agencia se ha completado con la publicación de diferentes entrevistas concedidas a diversos medios de comunicación.

3. Premios «Protección de Datos Personales»

Por medio de dos Resoluciones de 21 de enero de 2002, se convocaron los premios «Protección de Datos Personales» y de Periodismo «Protección de Datos Personales».

El Premio «Protección de Datos Personales» Convocatoria 2002, con una dotación de seis mil diez euros y un accésit con una asignación de mil quinientos dos euros, 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 «Transferencia internacional de datos personales» del que es autora doña Diana Sancho Villa. De esta obra se ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional.

La trabajo premiado realiza un minucioso análisis en relación con las Transferencias Internacionales de datos personales. Se trata de un estudio exhaustivo y muy documentado,

cuyo gran nivel de detalle no se opone a un análisis de amplia vocación general. Dicho trabajo incorpora una abundante bibliografía nacional y extranjera, analizando el tema que le da título desde la perspectiva de las diversas normas que resultan de aplicación. Asimismo, la obra analiza el sistema de la responsabilidad civil y el derecho sancionador derivados del incumplimiento de la normativa vigente sobre esta materia.

Se concedió un accésit a la obra titulada «El tratamiento de los datos personales en el ámbito sanitario: intimidad *«versus»* interés público. Especial referencia al sida, técnicas de reproducción asistida e información genética», de la que es autora doña Noelia de Miguel Sánchez. En ella se recoge un exhaustivo estudio de la protección de datos en el entorno sanitario, analizando la evolución de este tema desde sus orígenes hasta la actualidad, e incorporando el estudio de las disposiciones más novedosas en éste ámbito. La obra analiza los derechos del paciente frente al conocimiento de sus datos por el profesional sanitario, abordando cuestiones tales como la posible información a los familiares, o el tratamiento de los datos de personas con proyección pública.

El Premio de Periodismo «Protección de Datos Personales», con una dotación de mil quinientos euros, 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.

Abreviaturas utilizadas

AAPP Administraciones Públicas.

ACC Autoridad de Control Común encargada del control de la Unidad de Apoyo Técnico del SIS.

ACES Agrupación Catalana de Establecimientos Sanitarios.

ACM Asociación de Centrales de Medios.

ACRA Asociación Catalana de Recursos Asistenciales.

ADSL Técnica de codificación de la señal para su transmisión por redes de telecomunicaciones, que permite transmitir grandes cantidades de información sobre un par de cobre.

AEAP Asociación Española de Agencias de Publicidad.

AEAT Agencia Estatal de Administración Tributaria.

AECE Asociación Española de Comercio Electrónico.

AESC *Association of Executive Search Consultants, Europe*; Asociación de búsqueda de asesores ejecutivos.

AGEMDI Asociación de Agencias de Marketing Directo e Interactivo.

AIF Asociación Internacional del Fomento.

AMPE Asociación de Medios Publicitarios.

ANF Asociación Nacional de Fabricantes.

APD Agencia de Protección de Datos.

APIS *Advanced Passenger Information System.* Sistema avanzado de información de pasajeros.

APTICE Asociación para la Promoción de las Tecnologías de la Información y el Comercio Electrónico.

ASC-SIA Autoridad de Supervisión Común del SIA.

ASIMELEC Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones.

BOA Boletín Oficial de la Comunidad de Aragón.

BOC Boletín Oficial de la Comunidad Canaria.

BOCA Boletín Oficial de la Comunidad de Cantabria.

BOCL Boletín Oficial de la Comunidad de Castilla – León.

BOCM Boletín Oficial de la Comunidad de Madrid.

BOE Boletín Oficial del Estado.

BOJA Boletín Oficial de la Junta de Andalucía.

BOLR Boletín Oficial de la Comunidad de la Rioja.

BON Boletín Oficial de la Comunidad de Navarra.

BORM Boletín Oficial de la Región de Murcia.

CC Consejo Consultivo.

CCAA Comunidades Autónomas.

CCC Código de Cuenta Cliente.

CCI Centro de Cooperación Interbancaria.

CE Constitución Española.

CECIR Comisión Ejecutiva de la Comisión Interministerial de Retribuciones.

CEN/ISSS *Information Society Standardization System.* (Sistema de normalización de la sociedad de la información) del Comité Europeo de Normalización.

CIDSEP Centro Interdisciplinar de Derecho Social y Economía Política.

CIF Código de Identificación Fiscal.

CIRBE Central de Información de Riesgos del Banco de España.

CIRCA Página *Web* creada como consecuencia de los encuentros de las Autoridades de Control Europeas para el intercambio de información sobre reclamaciones internacionales.

CIS *Customs Information System* (acrónimo ingles del SIA). '

CJ–PD Grupo de Proyectos Sobre Protección de Datos.

CJ-PD-GC Grupo de Coordinación del CJ-PD

CNIL *Comissión Nationale de L'Informatique et des Libertes.* Autoridad competente en materia de protección de datos en Francia.

CNPD Comisión Nacional de Protección de Datos (Autoridad portuguesa de protección de datos).

CSIS Unidad de Apoyo Técnico Central del Sistema de Información Schengen.

CT Código Tipo.

DCS *Departure Control System* (sistema de control de salida).

DGS Dirección General de Seguros.

DNI Documento Nacional de Identidad.

DOCE Diario Oficial de las Comunidades Europeas.

DOCM Diario Oficial de la Comunidad de Castilla – La Mancha.

DOE Diario Oficial de Extremadura.

DOGA Diario Oficial de la Comunidad Gallega.

DOGC Diario Oficial de la Generalidad de Cataluña.

DOGV Diario Oficial de la Comunidad Valenciana.

EAPD Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos.

ENUM *Telephone Number Mapping*: Nuevo protocolo de asociación de números de teléfono a nombres de dominio en Internet.

EURODAC Reglamento (CE) para la comparación de las impresiones dactilares para la aplicación del Convenio de Dublín.

EUROJUST Órgano de la UE para la coordinación eficaz entre las autoridades nacionales encargadas de las actuaciones judiciales, y de ayuda a las investigaciones relativas a delincuencia organizada.

EUROPOL Oficina Europea de Policía.

EUROSTAT Oficina de Estadística de las Comunidades Europeas.

FECEMD Federación Española de Comercio Electrónico y Marketing Directo.

FEMP Federación Española de Municipios y Provincias.

FHSA Fichero Histórico de Seguros del Automóvil.

FIDE *Fichier d'Identification des Dossier d'Enquêtes*; Fichero de expedientes de investigación aduanera creado al amparo del convenio SIA.

FNEP Federación Nacional de Empresas de Publicidad.

FTC *Federal Trade Commission*; Comisión Federal del Comercio.

GPS Sistema de Posicionamiento Global.

GSM *Global System Mobile*; estándar tecnológico todavía vigente de la telefonía móvil europea.

GT29 Grupo de trabajo del artículo 29 de la Directiva 95/46

HC Historia Clínica.

ICANN *The Internet Corporation for Assigned Names and Numbers.*

IDS *Intrusion Detection System*; Sistema de detección de intrusiones.

IETF *Internet Engineering Task Force*; Grupo de Trabajo de Ingeniería de Internet.

IMEI *International Mobile Equipment Identifier*; Número que identifica un terminal móvil.

INAP Instituto Nacional de la Administración Pública.

INE Instituto Nacional de Estadística.

INSALUD Instituto Nacional de la Salud.

INSS Instituto Nacional de la Seguridad Social.

INTERPOL Organización Internacional de Policía Criminal.

IP *Internet Protocol*: Protocolo de transmisión de información por Internet.

IPAMED Registro de Incidencias-Pago Mediadores.

IPv6 *Internet Protocol Versión 6*; 6ª versión del IP

IRPF Impuesto sobre la renta de las personas físicas.

ITU *International Telecommunication Union*; Unión Internacional de Telecomunicaciones (UIT).

ITV Inspección Técnica de Vehículos.

IWGDPT Grupo Internacional de Protección de Datos en Telecomunicaciones.

LCAP Ley de Contratos de las Administraciones Públicas.

LOPD Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LORTAD Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

LSSI Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

NCSA Nuevo Concepto del Sistema de Análisis.

NIF Número de Identificación Fiscal.

NSIS Parte Nacional del Sistema de Información Schengen.

OCDE Organización para la Cooperación y el Desarrollo Económico.

OCUC Organización de Consumidores y Usuarios de Cataluña.

PET Técnica de Mejora de la Privacidad.

PNR *Passenger Name Record*; registro de nombres de pasajeros.

POEMAE Proyecto Operativo de los Estados miembros con apoyo de Europol.

PKI Infraestructura de Clave Pública.

PHARE Programa de la Comisión Europea para que los países candidatos se beneficien de la experiencia práctica directa de otros organismos similares de un Estado miembro.

RAI Registro de Aceptaciones Impagadas.

RGPD Registro General de Protección de Datos.

RP Práctica Recomendada.

SGAPD Secretaría General de la Agencia Protección de Datos.

SGID Subdirección General de Inspección de Datos.

SIA Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros.

SIS Sistema de Información Schengen.

SMS Protocolo para el servicio de envío de mensajes cortos.

SOLVIT Red de resolución de conflicto en el seno del Mercado Interior.

STC Sentencia del Tribunal Constitucional.

STS Sentencia del Tribunal Supremo.

T – PD Comité Consultivo del Convenio 108 del Consejo de Europa.

TC Tribunal Constitucional.

TID Tratamiento Informatizado o Digital de Datos.

TIREA Tecnologías de la Información y Redes para las Entidades Aseguradoras.

TS	Tribunal Supremo.
TSJ	Tribunal Superior de Justicia.
UE	Unión Europea.
UCH	Unión Catalana de Hospitales.
UNESPA	Unión Española de Entidades Aseguradoras y Reaseguradoras.
WHOIS	Herramienta informática que permite efectuar búsquedas a distancia en bases de datos de Internet.
WP	*Working Party*. Grupo de trabajo.

Anexos

Códigos Tipo

Código ético de comercio electrónico y publicidad interactiva

Preámbulo

Como es bien sabido, los orígenes de Internet se remontan a los años sesenta, y se encuentran en las actividades propias de un proyecto de investigación en el entorno universitario puesto en marcha por diversas agencias del gobierno de los Estados Unidos. Todo ello, sin olvidar la relevancia del papel desempeñado en el origen y la evolución de Internet por los trabajos desarrollados en los años ochenta en Europa, en concreto en el ámbito de la elaboración del protocolo de comunicaciones, por los Laboratorios Europeos de Física de Partículas (CERN), en Suiza por los científicos R.Carillau y T.Berners-Lee, que bautizaron un sistema de información global para el intercambio de datos esenciales para la comunidad científica como «world wide web» (www). No obstante, desde aquella primera época hasta nuestros días, Internet ha experimentado una vertiginosa evolución, cuya última etapa es, actualmente, el proyecto de convergencia tecnológica. Hoy en día, Internet constituye un eficaz medio para intercambiar y acceder a gran cantidad de información. De este modo, Internet se ha convertido en un nuevo medio de comunicación y de transacciones comerciales que ha dejado de ser una promesa de futuro, para pasar a convertirse ya en una realidad consolidada y con enormes potencialidades, constituyendo la punta de lanza de los medios electrónicos de comunicación a distancia.

En efecto, en los últimos años estamos asistiendo a un proceso de revolución tecnológica sin precedentes por la rapidez de su generalización entre los usuarios. Tanto empresas como consumidores hacen hoy en día un amplio uso de lo que se ha dado en conocer como «nuevas tecnologías», siendo posiblemente Internet el ejemplo más visible y característico de las

mismas. La expansión de estas tecnologías ha sido imparable hasta el momento, constituyendo en algún caso, como el de la telefonía móvil o el del propio Internet, un fenómeno imprevisible, planteando en muchos casos interrogantes ante los problemas de aplicabilidad de la regulación legal existente.

Sin embargo, lo más significativo de esta revolución está aún por llegar. La tendencia en la evolución de las tecnologías apunta siempre hacia un mismo camino, el marcado por la integración de sectores diferentes tradicionalmente separados, como el relativo a las telecomunicaciones o a los medios audiovisuales, en un proceso que se conoce como convergencia tecnológica. El reto para la regulación de este fenómeno es aún mayor, dada la confluencia de diferentes legislaciones sectoriales en ocasiones contradictorias entre si. Para solucionar este problema, tanto el legislador español como el comunitario proyectan la futura normativa atendiendo al principio de neutralidad tecnológica, conforme al cual la aplicabilidad de la norma no queda condicionada por el medio tecnológico empleado (Internet, telefonía...), por lo que las diferentes normativas sectoriales en función del medio o soporte tecnológico tienden a desaparecer o a fundirse en un único cuerpo legal.

Por ello, estamos ante un sector extremadamente dinámico y en permanente evolución, donde las posibilidades de obsolescencia normativa son mayores que en cualquier otro. Adaptarse a los cambios previendo soluciones a estos problemas de regulación es uno de los objetivos que inspiran el presente Código.

Los servicios ofrecidos a través de los medios electrónicos de comunicación a distancia son múltiples y muy variados. Abarcan una amplia variedad de actividades económicas remuneradas, de las que forman parte las transacciones contractuales, así como servicios no remunerados, como las comunicaciones comerciales.

Es evidente, por lo demás, que la publicidad que se difunde a través de Internet y otros medios electrónicos de comunicación a distancia queda sometida a las normas generales que regulan la actividad publicitaria. En la misma medida, las transacciones comerciales que se realizan a través de la red quedan, con carácter general, sujetas a las normas que ordenan estas transacciones en el mundo *off-line*. Aunque conviene aclarar que no resultan aplicables a estos nuevos medios tecnológicos las normas especiales promulgadas para determinados medios de comunicación como, por ejemplo, la televisión, es importante recordar que tanto la publicidad como las transacciones contractuales realizadas a través de medios electrónicos deberán respetar la legislación vigente en materia de protección de datos, cuyas líneas maestras están plasmadas, en nuestro país, en la Ley Orgánica 15/1999, de protección de datos de carácter personal (así como en sus normas de desarrollo, entre las que se encuentra el Real Decreto 994/1999, que desarrolla, con mayor detalle, las reglas aplicables en cuanto a las medidas de seguridad).

Así las cosas, el debate se centra, en gran medida, en determinar si Internet, y los restantes medios electrónicos de comunicación a distancia, como soportes publicitarios y medios de intercambios comerciales específicos, precisan también de normas especiales que regulen las comunicaciones comerciales y las transacciones contractuales que en la red se realizan con los consumidores. La respuesta, en principio, parece que debe ser afirmativa, toda vez que las características propias de estos medios pueden hacer necesaria una cierta adaptación de las normas generales en la materia, así como la adopción de normas específicas que contemplen y regulen supuestos de hecho que no se plantean en los restantes medios de comunicación. En todo caso, ya sea para aplicar las normas generales o las normas especiales por razón del medio, los nuevos medios electrónicos de comunicación a distancia requieren, dadas sus especiales características, del establecimiento de mecanismos de regulación y autorregulación nuevos o de la adaptación de los ya vigentes.

Las actuales tendencias en materia de ordenación de los medios electrónicos de comunicación a distancia, van claramente encaminadas hacia la senda de la corregulación. No en vano, y teniendo en cuenta los nada desdeñables retos jurídicos que la convergencia genera en lo que a la regulación de los nuevos medios se refiere, tanto los foros internacionales, como las instancias comunitarias y los legisladores nacionales ya han reconocido el valor y la eficacia de los mecanismos de autorregulación creados por la propia industria, y que sirven como complemento de los sistemas legales y jurisdiccionales de los diferentes países. Y en este sentido, ya son muchas las voces autorizadas que han expresado la necesidad de una adecuada promoción de los sistemas de autorregulación como imprescindible complemento de las tradicionales estructuras de Derecho para regular este nuevo medio y garantizar unos niveles elevados de seguridad jurídica y protección de los derechos de todas las partes implicadas. En efecto, en nuestro entorno más inmediato, que no es otro que el de la Unión Europea, el legislador comunitario ha recogido esta corriente en varias Directivas, como la 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales o la muy reciente Directiva 2002/58/CE sobre tratamiento de datos personales y protección de la intimidad en las comunicaciones electrónicas, así como la Directiva 2000/31/CE, de 8 de junio, sobre el comercio electrónico. Esta última realiza una firme apuesta por los sistemas de autorregulación, instando a los Estados miembros y a la Comisión a una decidida promoción y desarrollo de los mismos en su doble vertiente de elaboración de códigos éticos y de creación y consolidación de mecanismos extrajudiciales de resolución de controversias. En la misma línea se posiciona nuestra legislación nacional, con la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

En un entorno tan dinámico y cambiante como el de los medios electrónicos de comunicación a distancia, donde la capacidad de adaptación a los cambios tecnológicos, económicos o sociológicos es determinante, los sistemas de autorregulación presentan una serie de

ventajas respecto a los cauces convencionales de regulación y de resolución de controversias, tales como la rapidez de actuación y la flexibilidad, así como su vocación de integración y coordinación a nivel transnacional o supranacional, lo cual constituye una vía de superación de los problemas que la globalidad y la falta de territorialidad de la Red plantean para las legislaciones y tribunales nacionales. Son todos éstos aspectos sumamente importantes para un adecuado desarrollo de todas las potencialidades y beneficios que ofrecen estos nuevos medios y los servicios ofrecidos a través de los mismos.

En España contábamos ya con dos sistemas de autorregulación operativos para Internet: de un lado, el Código de Protección de Datos Personales en Internet, de la AECE, y de otro, el Código Ético de Publicidad en Internet, de Autocontrol de la Publicidad. Ambos sistemas contaban también con sus respectivos mecanismos de aplicación de tales normas éticas en caso de controversia. Cabían varias posibilidades para adaptar ambos sistemas a los avances tecnológicos y legales que se han producido desde su adopción, para dar respuesta así a la invitación a implementar sistemas de autorregulación que formula la Directiva de Comercio Electrónico y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). Con una clara voluntad de colaboración, ambas asociaciones (AECE y Autocontrol) decidieron que, tanto para los consumidores como para la industria y la sociedad en general, era más eficaz aunar los esfuerzos de ambas entidades para establecer un sistema de autorregulación integral que se beneficiara de las especializaciones y recursos respectivos. Con todo ello, además, se evitaba la aparición de diferentes sistemas de autorregulación dispersos con el riesgo de crear confusión en los consumidores y en el mercado.

A este propósito de aunar esfuerzos se sumó también el Interactive Advertising Bureau Spain (IAB Spain), que, en estrecha colaboración con Autocontrol, ha contribuido activamente en la redacción del presente Código, en todo lo que a la ordenación normativa de las comunicaciones comerciales se refiere. El resultado de esta colaboración se refleja en el texto de las normas éticas sobre comunicaciones comerciales de este Código, que, tomando el Código Ético sobre Publicidad en Internet de Autocontrol de 1999 como punto de partida, plasman el trabajo desarrollado en esta materia por el IAB Spain durante varios meses, a través de su Comisión de Legislación y Estándares.

Asimismo, a este proyecto de sistema de autorregulación integral para la publicidad y el comercio electrónicos se han adherido también otras asociaciones que desarrollan su actividad en el marco de las comunicaciones comerciales y los nuevos medios electrónicos de comunicación a distancia, tales como la Federación española de Comercio Electrónico y Marketing Directo (FECEMD), la Asociación de Agencias de Marketing Directo e Interactivo (AGEMDI), la Asociación Española de Anunciantes (ANUNCIANTES), la Asociación Española de Agencias de Publicidad (AEAP), la Federación Nacional de Empresas de Publicidad (FNEP), la Asociación de Centrales de Medios (ACM), la Asociación de Medios Publicitarios

(AMPE), y la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC).

Así las cosas, mediante el presente Código Ético de Publicidad y Comercio Electrónico, la Asociación Española de Comercio Electrónico (AECE) y la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), en su condición de organizadoras, así como IAB Spain, como colaboradora, y ANUNCIANTES, AEAP, AMPE, ACM, FECEMD, AGEMDI, FNEP y ASIMELEC, y otras asociaciones que deseen participar en este sistema de autorregulación, en calidad de entidades participantes, desean manifestar su serio compromiso por crear y sostener, en el marco de la defensa del ejercicio de la ética y deontología profesional, un sistema integral de autorregulación relativo a la publicidad y las transacciones comerciales con los consumidores en los medios electrónicos de comunicación a distancia.

Este sistema de autorregulación, con vocación de universalidad para todo el territorio español y de aunar las voluntades del mayor número de instancias profesionales dedicadas a la realización, fomento y defensa del desarrollo de la publicidad y el comercio en los nuevos medios, resulta comprensivo tanto de las comunicaciones comerciales, como de los aspectos contractuales derivados de las transacciones comerciales que las empresas realicen con los consumidores a través de Internet y otros medios electrónicos e interactivos. La protección de datos personales, por supuesto, queda también comprendida en el ámbito de regulación material del presente Código, siendo ésta un área que requiere de una adecuada salvaguarda en el desarrollo tanto de actividades publicitarias como de transacciones contractuales con los consumidores.

Entre las diversas opciones posibles, se ha escogido un sistema de autorregulación integral, tomando como modelo los sistemas de autorregulación desarrollados en los países de nuestro entorno cultural, básicamente la Unión Europea y los Estados Unidos de América, que comprenda los diferentes aspectos de las relaciones entre las compañías y los consumidores y usuarios —publicidad, transacciones comerciales y protección de datos—, con una especial atención a la protección de la infancia.

El presente sistema de autorregulación nace con la intención de desarrollar un importante papel, dado que presta un servicio de indudable valor tanto para la industria como para los consumidores. Los sistemas de autorregulación deben gozar de credibilidad entre la industria y los consumidores, y esta credibilidad vendrá determinada por la eficacia que demuestre como instrumento de resolución de controversias y de promoción de elevados niveles de corrección ética. Es por ello que se atiende la necesidad de que el sistema esté constituido por dos elementos básicos en todo sistema de autorregulación: de un lado, un código de conducta, en el que se recogen las normas que los miembros adheridos al sistema se comprometen a observar y cumplir, y de otro lado, un mecanismo de control de la aplicación de

tales normas, que reúne expertos independientes e imparciales, con competencia para resolver las eventuales reclamaciones y controversias que pudieran surgir. Este sistema de resolución de conflictos está inspirado en los principios de independencia, transparencia, contradicción, eficacia, legalidad, libertad de elección y derecho de representación por parte del consumidor, que coinciden plenamente con los principios exigidos por las autoridades comunitarias para el reconocimiento de los mecanismos extrajudiciales de resolución de controversias con los consumidores, plasmados en la Recomendación 98/257/CE de la Comisión Europea.

La sinergia creada entre las asociaciones organizadoras del nuevo sistema de autorregulación de la publicidad y el comercio electrónico rentabilizará, sin sustituirlos, instrumentos de autodisciplina ya existentes y que han probado sobradamente su eficacia, como el Jurado de la Publicidad de Autocontrol o la Secretaría de ambas asociaciones. También, y para evitar duplicidades, el nuevo Código que ahora se presenta sustituirá los códigos específicos que dichas asociaciones habían adoptado para regular aspectos concretos de Internet (publicidad y protección de datos personales), que quedarán derogados con la adopción del presente.

Otro de los motivos que subyace en el lanzamiento de este sistema integral de autorregulación para el comercio electrónico es el de generar confianza en los consumidores, elemento de capital importancia. Por ello, las empresas que se adhieran al sistema deben poder mostrar a sus eventuales clientes que pertenecen al mismo, de forma que el consumidor conozca el sistema de protección de los derechos e intereses del usuario que se pone a su servicio. Es preciso que exista un mecanismo de acreditación de la adhesión al sistema de autodisciplina, de forma que sean identificadas las empresas comprometidas activamente en su sostenimiento y desarrollo. Para atender esta necesidad de forma adecuada, se ha configurado un sello acreditativo que certifica la adhesión al sistema, si bien este sello no implica una verificación previa de las ofertas de la compañía poseedora de la identificación, sino su compromiso de respeto a las normas de conducta recogidas en el Código en el desarrollo de su actividad comercial, y de cumplido acatamiento de las resoluciones que el organismo de resolución de controversias adopte como consecuencia de las eventuales reclamaciones que se puedan presentar.

Es por todo ello que el sistema que ahora se presenta cuenta básicamente con cuatro elementos. A saber:

1. Un conjunto de normas deontológicas, que son las recogidas en este Código Ético sobre Comercio electrónico y Publicidad Interactiva. Dos son las grandes áreas de regulación material en que se divide este Código: comunicaciones comerciales y comercio electrónico, sin olvidar la necesaria atención que merece la protección de datos personales en el desarrollo de ambas actividades, así como la protección y salvaguarda de los

menores. El Título atinente a las comunicaciones comerciales recoge las normas sobre «Publicidad Interactiva» elaboradas por IAB Spain, que pasan así a integrarse en este cuerpo de normas éticas de vocación más amplia, y cuya aplicación IAB Spain encomienda al Jurado de la Publicidad de Autocontrol. El Título dedicado al comercio electrónico, fundamentalmente elaborado por AECE, y movido por una clara vocación de permanencia, ha tratado de evitar normas excesivamente casuísticas —ineficaces en un ámbito tan dinámico y cambiante como éste—, estableciendo principios y reglas de conducta generales, que resultan exigibles a los operadores en sus transacciones con los consumidores para la contratación de bienes y servicios a través de medios electrónicos de comunicación a distancia, con el fin de dar adecuada respuesta a la necesidad de mantener altos niveles de protección de sus derechos e intereses. Como queda patente en el texto del Código, la protección de datos personales y la protección de los menores son áreas de indudable y necesario interés, a las que, no en vano, el Código dedica sendos Títulos.

2. Un sistema de aplicación de esas reglas que resuelva, bajo los principios de independencia, transparencia, contradicción de las partes, eficacia, legalidad, libertad y representación, las controversias y reclamaciones que se presenten por eventuales incumplimientos de las reglas o normas mencionadas en el apartado anterior. Este sistema se basa en la actividad de dos mecanismos o sistemas de control que cumplen con los principios plasmados en la Recomendación 98/257/CE de la Comisión Europea, encargados de resolver las eventuales controversias que se pudieran plantear por el pretendido incumplimiento de las normas del Código: el Jurado de la Publicidad, para todas las cuestiones relacionadas con las comunicaciones comerciales, y la Junta Arbitral Nacional de Consumo, para las cuestiones de carácter contractual con los consumidores que se puedan suscitar, previo intento de mediación por parte de AECE. El primero, en funcionamiento desde hace más de cinco años, depende de Autocontrol de la Publicidad, y el 25% de sus miembros son nombrados de común acuerdo con el Instituto Nacional de Consumo, de acuerdo con lo dispuesto en el Convenio suscrito en enero de 1999 entre dicho organismo y Autocontrol de la Publicidad; el segundo, en funcionamiento desde hace más de ocho años de conformidad con el Real Decreto 636/1993, de 3 de mayo, por el que se regula el Sistema Arbitral de Consumo, encomienda a un Colegio Arbitral la resolución de las controversias, con el sometimiento voluntario de las dos partes en conflicto, y sus pronunciamientos tienen la eficacia de un laudo arbitral.

3. El funcionamiento cotidiano de este mecanismo bicéfalo de resolución de controversias será apoyado por una Secretaría, que asegurará la adecuada coordinación y eficacia en la tramitación de las reclamaciones que se reciban, impulsando y coordinando el procedimiento ante los dos órganos antes citados. La Secretaría, dirigida conjuntamente por los Directores Generales de AECE y AUTOCONTROL se encargará asimismo

de la asignación y administración cotidiana del sello de confianza, de la gestión económica del sistema, así como de la elaboración de estadísticas y la adecuada promoción del sistema de autorregulación.

4. Un sello de confianza que permita identificar las empresas y compañías adheridas a este sistema de autorregulación, que será gestionado por la Secretaría del sistema[1].

Todo ello, en el marco del más absoluto respeto a la legalidad vigente y, en especial sobre la base de lo previsto en los artículos 16 «Códigos de conducta» y 17 «Solución Extrajudicial de litigios» de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de la Unión Europea, de 8 de Junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, conocida como Directiva de Comercio Electrónico, así como de los artículos 18 y 32 de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

La gestión y financiación del sistema de autorregulación serán aseguradas por las asociaciones organizadoras (AECE y AUTOCONTROL). Dichas asociaciones establecerán, conjuntamente, la forma en que las entidades participantes y las compañías adheridas al sistema contribuirán a su sostenimiento económico.

Junto a las asociaciones organizadoras del sistema integral de autorregulación del comercio electrónico y la publicidad interactiva —la Asociación Española de Comercio Electrónico (AECE) y la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL)—, participan en este sistema de autorregulación el Interactive Advertising Bureau Spain (IAB Spain), en calidad de entidad colaboradora, y, como asociaciones participantes, la Federación Española de Comercio Electrónico y Marketing Directo (FECEMD), la Asociación de Agencias de Marketing Directo e Interactivo (AGEMDI), la Asociación Española de Anunciantes (ANUNCIANTES), la Asociación Española de Agencias de Publicidad (AEAP), la Federación Nacional de Empresas de Publicidad (FNEP), la Asociación de Centrales de Medios (ACM), la Asociación de Medios Publicitarios (AMPE) y la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), y demás asociaciones que deseen participar en este sistema de autorregulación, así como otras organizaciones representativas del sector que decidieran participar en el mismo en un futuro.

---

[1] ***Este sello de confianza será completado o complementado con el sello elaborado por el Gobierno cuando éste sea creado.*** Este inciso se inspira en el texto de la LSSI:
«Disposición Final Cuarta («Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías»). En el plazo de un año desde la entrada en vigor de esta Ley, el Gobierno aprobará un distintivo que permita identificar a los prestadores de servicios que respeten Códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros requisitos, la adhesión al Sistema Arbitral de Consumo (...)».

Todas ellas, en reunión conjunta celebrada al efecto en Madrid, el día 28 de octubre de 2002, se comprometen a promover este sistema de autorregulación entre sus miembros y a darlo a conocer y difundirlo tanto en los distintos sectores empresariales relacionados como en la sociedad española en general —especialmente entre los usuarios de Internet y de otros medios electrónicos e interactivos, y entre las diferentes Administraciones Públicas—, así como a atenerse a lo previsto en el presente Código y a acatar las resoluciones dictadas por los órganos de resolución de controversias encargados de la supervisión del control y aplicación del Código.

El presente Código ha sido sometido a la consulta de la Agencia de Protección de Datos, el Ministerio de Ciencia y Tecnología y el Instituto Nacional de Consumo. Asimismo, se ha procedido a la inscripción del Código en el Registro General de Protección de Datos de la Agencia de Protección de Datos.

Considerando el dinamismo de este sector y el rápido e imprevisible desarrollo de la evolución tecnológica, las normas contenidas en este Código deberán ser revisadas periódicamente, para garantizar su actualidad. Asimismo, en este contexto, las asociaciones organizadoras promoverán, en estrecha colaboración con la Agencia de Protección de Datos, la elaboración de anexos o complementos al presente Código en los que se contemplen procedimientos estandarizados que faciliten el cumplimiento de los principios y derechos aplicables en materia de protección de datos, adaptados a las peculiaridades de las empresas adheridas.

De igual forma, considerando la globalidad y extraterritorialidad implícita de la *world wide web* y de los nuevos medios electrónicos e interactivos, este Código y los mecanismos de autocontrol establecidos para su aplicación tienen vocación de integración y/o coordinación en futuros sistemas internacionales de autorregulación para Internet y los servicios de la sociedad de la información, cuando sean una realidad.

Título I. Definiciones y ámbito de aplicación

Artículo 1. Definiciones

A los efectos del presente Código, debe entenderse por:

a) **Medios electrónicos de comunicación a distancia:** todos aquéllos que permitan la prestación de servicios de la sociedad de la información.

No tendrán la consideración de medios electrónicos de comunicación a distancia, a los efectos de este Código, los que no reúnan las características arriba expresadas, y, en particular, los siguientes:

— la telefonía vocal, fax o télex,
— el correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan,
— la radiodifusión televisiva,
— la radiodifusión sonora,
— el teletexto televisivo.

b) **Publicidad:** toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones.

No se considerará publicidad a los efectos de este Código:

— los datos que permiten acceder directamente a la actividad de una empresa, organización o persona, y concretamente el nombre de dominio o la dirección de correo electrónico.
— las comunicaciones comerciales relativas a los bienes servicios o a la imagen de dicha empresa, organización o persona, elaboradas de forma independiente de ella, en particular cuando estos se realizan sin contrapartida económica.
— la comunicación bilateral individualizada originada por solicitud del usuario.
— los contenidos editoriales de las páginas web, entendiendo por tales todos aquéllos que no estén orientados a la promoción, directa o indirecta, de la contratación de bienes, servicios, derechos y obligaciones.

c) **Anunciante:** la persona física o jurídica en cuyo interés se realiza la publicidad.

d) **Destinatarios:** las personas a las que se dirija o alcance la publicidad.

e) **Comercio electrónico:** toda transacción económica consistente en la contratación de productos y/o servicios entre un oferente y un consumidor, en la que la oferta por parte del oferente y la aceptación por parte del consumidor se realizan enteramente a través de un medio electrónico de comunicación a distancia.

f) **Oferente:** persona física o jurídica, pública o privada que, en el ejercicio habitual de una actividad económica, realiza una oferta de comercio electrónico a consumidor/es.

g) **Consumidor:** a los efectos de la contratación por medios electrónicos, se entenderá por consumidor toda persona física o jurídica que utiliza o disfruta como destinatario final

los productos y/o servicios contratados con un oferente. No será considerado consumidor aquél que, sin constituirse en destinatario final, adquiera o contrate y utilice o consuma productos y/o servicios con el fin de integrarlos en procesos de producción, transformación, comercialización o prestación a terceros.

h) **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Se considerarán datos personales, entre otros, la dirección personal de correo electrónico y el número de teléfono, siempre que permitan identificar a su titular.

Artículo 2. Ámbito de aplicación

El presente Código será aplicable a la publicidad y al comercio electrónico realizados a través de medios electrónicos de comunicación a distancia, por personas físicas o jurídicas con establecimiento permanente en España o dirigidos de forma específica al mercado español.

Título II. Publicidad

Capítulo I. Normas Generales

Artículo 3. Principios generales

1. La publicidad en medios electrónicos de comunicación a distancia deberá ser conforme a la ley aplicable, decente, honesta y veraz, en los términos en que estos principios han sido desarrollados por el Código de Conducta Publicitaria de Autocontrol [link activo] y por el Código de Práctica Publicitaria de la Cámara Internacional de Comercio [link activo].

2. La publicidad en medios electrónicos de comunicación a distancia deberá respetar las normas recogidas en los Códigos mencionados en el párrafo anterior, así como aquellas otras que se recojan en los Códigos sectoriales contemplados en el artículo 8 del Código de Conducta Publicitaria de Autocontrol.

3. La publicidad en medios electrónicos de comunicación a distancia deberá ser elaborada con sentido de la responsabilidad social, y no deberá constituir nunca un medio para abusar de la buena fe de sus destinatarios, evitando así que pueda deteriorarse la confianza del público en estos medios.

4 La publicidad en medios electrónicos de comunicación a distancia no tendrá contenidos que atenten contra la dignidad de la persona, o sean discriminatorios (por razón de nacionalidad, raza, sexo, orientación sexual, convicciones religiosas o políticas, o cualquier otra circunstancia personal o social), o que inciten a la comisión de actos ilícitos.

Artículo 4. Identificación del Anunciante

En la publicidad en medios electrónicos de comunicación a distancia el anunciante deberá ser siempre identificable, de forma tal que sus destinatarios puedan reconocerlo y ponerse en contacto con él sin dificultades. A estos efectos, el anunciante deberá indicar a sus destinatarios, de forma clara, directa y fácilmente accesible, su nombre o denominación social, su domicilio a efectos legales así como su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

Artículo 5. Identificación de la publicidad

La publicidad en medios electrónicos de comunicación a distancia será fácilmente identificable como tal. No se admitirá la publicidad encubierta.

Artículo 6. Información al destinatario

1. Además de la información recogida en el artículo 4 sobre la identificación del anunciante, éste deberá proporcionar a sus destinatarios, de forma clara y fácilmente accesible, todas aquellas informaciones que resulten exigibles de acuerdo con la legislación vigente.

2. Los anunciantes deberán informar del coste o precio de acceder a un mensaje o servicio cuando aquél sea mayor que el de las tarifas básicas de telecomunicación. Los destinatarios serán informados de tales costes antes de acceder al mensaje o servicio, de forma clara, y deberán disponer de un plazo de tiempo razonable y suficiente para poder desconectarse del servicio sin incurrir en gastos.

3. Las ofertas deberán identificarse de modo que el que las recibe pueda reconocerlas como ofertas. Si en la publicidad se presenta o realiza una oferta directa de contratación, se deberá proporcionar al destinatario una información clara, completa y precisa sobre el contenido y el alcance de aquélla. En todo caso, las informaciones a que se refiere el artículo 14 deberán resultar perfectamente visibles para el consumidor, y deberán ser exactas y susceptibles de prueba.

Artículo 7. Promociones publicitarias

1. A los efectos de este Código, se entenderá por promoción publicitaria toda técnica de promoción de ventas que, durante un periodo limitado de tiempo, ofrezca a sus destinatarios un valor añadido consistente en una ventaja económica o en cualquier otro tipo de incentivo material o inmaterial.

2. Las promociones publicitarias en medios electrónicos de comunicación a distancia deberán responder a los principios que rigen la publicidad en general, especialmente los de legalidad, veracidad y buena fe, sin que puedan constituir nunca un medio para abusar de la buena fe de sus destinatarios, ni explotar su posible falta de experiencia o conocimientos.

Artículo 8. Competencia desleal y respeto de los derechos de propiedad industrial e intelectual

1. La publicidad en medios electrónicos de comunicación a distancia deberá respetar los derechos de propiedad intelectual e industrial de terceras personas distintas del anunciante. En particular, en Internet, no se admite la introducción en el código fuente de nombres ocultos (metanames) que coincidan con marcas, nombres, rótulos o denominaciones de empresas o servicios sobre los que no se ostente la titularidad o una autorización de uso.

2. La publicidad en medios electrónicos de comunicación a distancia no deberá constituir nunca un medio de competencia desleal.

Capítulo II. Normas Especiales

Artículo 9. Publicidad enviada mediante mensajes de correo electrónico u otros medios de comunicación individual equivalentes

1. No se admitirá el envío de publicidad mediante mensajes de correo electrónico u otros medios de comunicación individual equivalentes por parte del anunciante cuando no haya sido solicitada o autorizada expresamente por el destinatario.

2. Se entiende concedida la autorización prevista en el párrafo anterior cuando, al tiempo de recabar los datos, se haya informado debidamente al destinatario sobre la posibilidad de envío publicitario y éste haya otorgado su consentimiento. En particular, se entiende que este consentimiento se consigue a través del procedimiento de listas de inclusión voluntarias (opt-in), aunque son igualmente admisibles otras prácticas que garanticen la prestación del consentimiento.

3. Aquellos anunciantes que utilizan mensajes por correo electrónico u otros medios de comunicación individual equivalentes con fines publicitarios deberán informar con claridad al destinatario sobre la posibilidad de notificar su deseo de no recibir ofertas posteriores y proporcionarle un mecanismo sencillo y de fácil acceso a través del cual el usuario pueda ejercitar este derecho de revocación de su consentimiento.

4. En todo caso, los mensajes publicitarios enviados por correo electrónico u otros medios equivalentes deberán identificarse claramente como tales, revelando asimismo la identidad del anunciante.

Artículo 10. Publicidad en grupos de noticias, foros, charlas (chats) y similares

1. No podrán utilizarse los grupos de noticias, tablón de anuncios o foros o charlas para enviar publicidad en línea (on-line), salvo que, en este último caso, previamente se haya obtenido el consentimiento del moderador del punto de encuentro o, en su defecto, del proveedor del servicio, o se ajuste a las reglas de admisión de publicidad establecidas para ese grupo, foro, charla o similar.

2. Se excluyen de lo previsto en este artículo, los foros o charlas de naturaleza publicitaria.

Artículo 11. Publicidad en la world wide web

1. La publicidad en la world wide web no podrá impedir la libre o normal navegación del usuario en Internet.

2. En particular, los mensajes publicitarios que reciba el usuario durante su navegación por una página web deberán permitirle en todo momento salir del mensaje publicitario o eliminarlo de su pantalla, volviendo a la página de origen desde la que el usuario accedió al mensaje publicitario.

Artículo 12. Patrocinio

1. Se entenderá por patrocinio cualquier contribución realizada por una entidad pública o privada a la financiación de páginas web u otros servicios prestados a través de medios electrónicos de comunicación a distancia, con la finalidad de promover su nombre, marca, imagen, actividades o productos.

2. Las web o servicios patrocinados deberán cumplir los siguientes requisitos:
   — El contenido editorial no podrá, en ningún caso, ser influido por el patrocinador de tal forma que se atente contra la responsabilidad y la independencia editorial del titular de la página o servicio.
   — Deberán estar claramente identificadas como tales, e incluirán el nombre, logotipo, marca, servicios u otros signos del patrocinador al principio o al final de la página web o servicio, o en los dos momentos.

También podrá identificarse al patrocinador por los medios antes mencionados en el desarrollo de la página o servicio patrocinado, siempre que ello se haga de forma esporádica y sin perturbar su lectura.

Título III. Comercio electrónico

Artículo 13. Principio de legalidad

Las actividades de contratación de bienes o servicios con consumidores realizadas a través de medios electrónicos de comunicación a distancia deben respetar la normativa legal vigente y, de manera especial, los valores, derechos y principios reconocidos en la Constitución.

Artículo 14. Obligaciones previas al inicio del procedimiento de contratación

1. Los oferentes que realicen transacciones comerciales con los consumidores a través de medios electrónicos de comunicación a distancia, deberán informar claramente sobre los pasos a seguir para la adquisición del bien o la contratación de servicio ofrecido.

2. Con anterioridad a la adquisición del bien o la contratación del servicio, y sin perjuicio de las obligaciones de información recogidas en el artículo 6 de este Código, el oferente deberá facilitar al consumidor el acceso a las condiciones generales de contratación aplicables en cada caso, para que las pueda consultar, archivar e imprimir. Asimismo, el oferente deberá informar al consumidor, de forma visible, acerca de, como mínimo, los siguientes extremos:
   a) Precio de compra completo, con referencia a los impuestos aplicables incluidos, así como la moneda, la modalidad de pago, el franqueo y los portes.

b) Plazo de validez de la oferta, si se tratase de una oferta promocional.
c) Términos, condiciones y formas de pago, incluyendo en su caso opciones de crédito.
d) Las diferentes modalidades de entrega o ejecución que puedan existir de los productos o servicios contratados
e) Características de los bienes o servicios y, en su caso, condiciones necesarias para su utilización.
f) Existencia o inexistencia de costes adicionales.
g) Condiciones para el ejercicio de los derechos de desistimiento y devolución, cancelación o cambios del correspondiente producto o servicio.
h) Garantías aplicables a la adquisición del producto o servicio.
i) Lugar y forma de presentación de posibles reclamaciones.
j) Domicilio del oferente a efectos legales.

3. En el momento inmediatamente anterior a la aceptación o prestación del consentimiento para la adquisición del bien o la contratación del servicio, el consumidor tendrá derecho a revisar un resumen en el que se incluyan, como mínimo, la relación de los productos que ha solicitado o de los servicios que desea contratar, así como las características esenciales de los mismos y las condiciones de compra o contratación, su importe total, el método de pago elegido, los impuestos aplicados y, en su caso, la forma y gastos de envío. Además, el consumidor deberá poder archivar e imprimir dicho resumen.

Artículo 15. Obligaciones de información posteriores a la celebración del contrato

1. Inmediatamente después de la aceptación por el consumidor de la adquisición del bien o la contratación del servicio, el oferente deberá enviarle un acuse de recibo, o facilitarle la descarga o impresión de un documento justificativo de la adquisición o contratación realizada, que contenga los datos relativos al contrato efectuado.

2. Una vez celebrado el contrato, el consumidor tendrá derecho a solicitar información sobre el estado en que se encuentra la entrega del bien o la prestación del servicio contratado, en la medida en que la naturaleza del bien o servicio contratado lo permita. Para ello, el oferente deberá informarle a través de la pantalla, del correo electrónico, del teléfono, u otro/s medio/s equivalente/s.

Artículo 16. Plazos de entrega

Si el oferente se encuentra en la imposibilidad de enviar o prestar los productos o servicios contratados dentro del plazo indicado en el contrato, deberá notificar esta circunstancia al

consumidor, informándole del nuevo plazo en el que aquél/los estarán disponibles. En este caso el consumidor tendrá la posibilidad de rescindir el contrato y pedir que se le reembolse el importe del producto o servicio si lo hubiese pagado.

Artículo 17. Desistimiento y devolución

1. El consumidor dispondrá de un período de reflexión, cuya duración será como mínimo la establecida en la normativa aplicable, durante el que podrá devolver el producto o servicio contratado sin penalización alguna. El oferente deberá indicar con claridad si los gastos relativos al coste directo de la devolución del producto o servicio contratado son soportados por él o si, por el contrario, recaen sobre el consumidor, así como el resto de condiciones de devolución de los productos o servicios contratados.

2. Este derecho de desistimiento y devolución no será de aplicación a los productos o servicios que puedan ser reproducidos o copiados con carácter inmediato, a aquéllos cuyo precio esté sujeto a fluctuaciones de un mercado no controlado por la empresa oferente, a los destinados a la higiene corporal, a aquéllos que por su naturaleza no puedan ser devueltos, y a todos aquéllos para los que la normativa aplicable prevea tal excepción.

3. En caso que el consumidor devuelva en perfecto estado el producto o servicio previamente contratado, con el documento justificativo del contrato y en los plazos establecidos en el mismo, tiene derecho a escoger entre el reembolso de las cantidades satisfechas o la sustitución del producto o servicio contratado por otro.

4. El oferente deberá establecer los mecanismos necesarios para facilitar al consumidor con el que han contratado el ejercicio de su derecho de desistimiento y la correspondiente devolución del producto o servicio.

Artículo 18. Servicio de atención al cliente

1. Los oferentes pondrán a disposición de los consumidores con los que han contratado un servicio interno de atención al cliente que resolverá las cuestiones o dudas que le puedan surgir al consumidor en un momento previo a la contratación de un bien o servicio, y que además atenderá las consultas o quejas que se le planteen posteriormente, que deberán ser respondidas en el plazo de tiempo más breve posible.

2. Los oferentes deberán proporcionar a los consumidores, de forma clara y suficiente, los datos necesarios para establecer un contacto rápido, personal y directo con el departamento o persona encargada de atender las posibles dudas o quejas que se planteen, así como del horario comercial de atención al cliente.

3. Los oferentes deberán guardar un registro en soporte duradero donde se recojan las quejas presentadas por los consumidores con los que haya contratado y las diversas circunstancias ocurridas en relación con cada una de dichas quejas.

Artículo 19. Seguridad y medios de pago

1. Los oferentes deberán proporcionar a los consumidores mecanismos de pago sencillos y seguros, y realizar todos los esfuerzos necesarios para mantenerse al día sobre los avances en este campo.

2. Los oferentes deberán adoptar sistemas de seguridad apropiados y dignos de confianza para salvaguardar la seguridad, integridad y confidencialidad de las transacciones financieras y pagos realizados por los consumidores. Estos deberán ser informados con claridad, antes de concluir la celebración del contrato, sobre el nivel de protección que se aplica a sus datos financieros y las posibles limitaciones de los sistemas de seguridad empleados. El oferente deberá informar al consumidor de la forma más transparente, clara y sencilla posible sobre la seguridad de los medios de pago y la tecnología que se esté utilizando para proteger las transmisiones, procesamiento y/o almacenamiento de sus datos financieros.

Título IV. Protección de datos personales

Artículo 20. Principios generales

1. Las empresas que realicen publicidad o transacciones contractuales con consumidores a través de medios electrónicos de comunicación a distancia deberán respetar la legislación vigente en materia de protección de datos personales.

2. Los datos de carácter personal sólo podrán obtenerse para su 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. Serán cancelados cuan-

do hayan dejado de ser necesarios o pertinentes para dicha finalidad, o cuando lo solicite el titular en el ejercicio de su derecho de cancelación.

3. Las empresas adheridas a este Código deberán respetar la privacidad de los usuarios, así como asegurar el secreto y seguridad de los datos personales, adoptando para ello las medidas técnicas y organizativas necesarias, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos.

4. Las empresas adheridas a este Código deberán apoyar iniciativas para ayudar a educar al consumidor sobre cómo proteger su intimidad en los medios electrónicos de comunicación a distancia.

Artículo 21. Obtención de los datos

1. Se prohibe la recogida de datos personales por medios fraudulentos, desleales o ilícitos.

2. Cuando las empresas adheridas a este Código recaben datos personales a través de medios electrónicos de comunicación a distancia, deberán informar previamente a los titulares, de forma inequívoca y claramente perceptible, de los siguientes extremos:
   - Existencia de un fichero o tratamiento de datos de carácter personal, finalidad de la recogida y destinatarios de la información.
   - Código o número de inscripción del (responsable del) fichero en el Registro de la Agencia de Protección de Datos.
   - Carácter obligatorio o facultativo de la respuesta a las preguntas que en su caso les sean planteadas, así como de las consecuencias de la obtención de los datos o la negativa a suministrarlos.
   - Posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
   - Identidad del responsable del tratamiento de los datos, y dirección (postal y de correo electrónico) que facilite la comunicación con el mismo.

3. Cuando los datos de carácter personal no hayan sido recabados del titular, éste deberá ser informado de forma expresa, precisa e inequívoca de la procedencia de los datos, así como de los extremos contenidos en el apartado 2 anterior, dentro de los tres meses siguientes al registro de los datos, salvo que ya hubiese sido informado de los mismos con anterioridad.

4. Cuando los datos hayan sido obtenidos de una fuente accesible al público y se destinen a la actividad de publicidad o prospección comercial, en cada comunicación deberá informarse al titular del origen de los datos, de la identidad del responsable de su

tratamiento, de la finalidad de su obtención y tratamiento, y de los derechos que asisten al titular de los mismos.

5. Las empresas que se anuncian en Internet y que recaben, capturen y traten datos personales, deberán informar a los consumidores, mediante un aviso en su web, de dicho tratamiento. De esta forma, el consumidor podrá, si lo desea, ejercitar su derecho de oposición, tanto en lo que se refiere a la captación como al tratamiento y transferencia de los datos.

6. Los datos de carácter personal sólo podrán ser cedidos a terceros cuando tenga relación directa con el cumplimiento de los fines del cedente y el cesionario. Será preciso contar con el consentimiento del titular, que deberá conocer de forma clara y precisa la finalidad a que se destinarán o el tipo de actividad del cesionario de los datos.

Artículo 22. Consentimiento del titular

1.- Se entenderá por consentimiento del titular toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que éste consienta el tratamiento de datos personales que le conciernen.

2. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del titular, salvo en los siguientes supuestos:
   — cuando se refieran a las partes de un contrato o pre-contrato de una relación negocial y sean necesarios para su mantenimiento o cumplimiento.
   — cuando los datos figuren en una fuente accesible al público y su tratamiento sea necesario para la satisfacción del interés legitimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del titular.

3. El consentimiento podrá ser revocado cuando exista una causa justificada para ello y no se le atribuyen efectos retroactivos.

Artículo 23. Ejercicio de derechos

1. Las empresas adheridas a este código deberán garantizar a los titulares el ejercicio de los derechos de acceso, rectificación y cancelación de sus datos personales, así como el derecho a oponerse al tratamiento y/o transferencia de los mismos, poniendo para ello a su disposición mecanismos de utilización sencillos (como dirección de correo electrónico y postal).

2. En ningún caso, las empresas podrán utilizar la información para finalidades distintas de las que haya consentido el consumidor, salvo que, previamente, le hayan advertido de la intención de hacerlo otorgándole un plazo y un procedimiento razonables para oponerse.

Artículo 24. Uso de cookies y dispositivos similares

1. Las cookies son pequeños ficheros de datos generados a través de instrucciones enviadas por los servidores web a los programas navegadores de los usuarios, y que se guardan en un directorio específico del terminal de aquéllos, con el objetivo de reunir información compilada por el propio fichero

2. Las empresas adheridas a este Código proveerán a los usuarios de información clara y comprensible sobre la presencia y la finalidad de las cookies u otros dispositivos o técnicas similares, poniendo a su disposición mecanismos sencillos y gratuitos para informarles sobre cómo desactivarlas. Asimismo, se avisará de forma clara cuándo queda imposibilitado el acceso o la utilización de un servicio interactivo por ser necesario el envío e instalación de cookies u otros dispositivos o técnicas similares en el terminal del usuario.

3. Las cookies u otras técnicas se utilizarán de forma disociada y nunca individualizada o relacionada a los datos personales de los usuarios, de forma que la información que se obtenga no pueda asociarse a persona identificada o identificable, salvo que el consumidor haya dado su consentimiento. En particular, cuando se utilicen cookies o pixels transparentes u otras técnicas asimilables, se proporcionará a los usuarios información clara y comprensible sobre su objetivo y de su utilización desvinculada de cualquier dato de carácter personal.

4. El tratamiento de las cookies es extrapolable por analogía a otras técnicas de monitorización de la conducta de los usuarios en su utilización de medios electrónicos de comunicación a distancia.

Artículo 25. Captación de datos personales en grupos de noticias, foros, charlas (chats) y similares con finalidad publicitaria

No podrán utilizarse los grupos de noticias, tablón de anuncios o foros o charlas para captar datos con finalidad publicitaria, salvo que dicha recogida se ajuste a las normas de obtención de datos establecidas en el presente Código.

Artículo 26. Seguridad y protección de datos

Las empresas adheridas a este Código deberán adoptar las medidas de seguridad apropiadas para salvaguardar la integridad y confidencialidad de los datos personales recabados, tratados y/o almacenados y realizar todos los esfuerzos necesarios para mantenerse al día sobre los avances en este campo. Los consumidores deberán ser informados, sobre el nivel de protección que se aplica a sus datos personales y las posibles limitaciones de los sistemas de seguridad empleados. El oferente deberá informar al consumidor de la forma más transparente, clara y sencilla posible sobre la tecnología que se esté utilizando para proteger las transmisiones, procesamiento y/o almacenamiento de sus datos personales.

Título V. Protección de menores

Artículo 27. Publicidad y protección de menores

La publicidad difundida en medios electrónicos de comunicación a distancia no deberá perjudicar moral o físicamente a los menores y tendrá, por consiguiente, que respetar los siguientes principios:

a) Deberá identificar los contenidos dirigidos únicamente a adultos.
b) No deberá incitar directamente a los menores a la compra de un producto o servicio, explotando su inexperiencia o su credulidad, ni a que persuadan a sus padres o tutores, o a los padres o tutores de terceros, para que compren los productos o servicios de que se trate.
c) En ningún caso deberá explotar la especial confianza de los niños en sus padres o tutores, profesores u otras personas.
d) No deberá, sin motivo justificado, presentar a los niños en situaciones peligrosas.

Artículo 28. Tratamiento de datos de menores

1. Para recoger datos o comunicarse con menores a través de medios de comunicación electrónica, las empresas adheridas a este Código deberán tener en cuenta la edad, el conocimiento y la madurez de su público objetivo. En ningún caso podrán recabarse del menor datos relativos o relacionados con la situación económica o la intimidad de los otros miembros de la familia.

2. Las empresas adheridas a este Código deberán alentar a los menores a obtener autorización de sus padres o tutores antes de facilitar información en línea (on-line), y establecer mecanismos que aseguren que los niños han obtenido el consentimiento de aquéllos.

3. Los padres o tutores podrán oponerse al envío de publicidad o información solicitada por los menores a su cargo, dirigiéndose para ello al responsable del fichero mediante un sistema que asegure su identidad.

4. Además del respeto a la opción de los padres de limitar la recogida de estos datos online, las empresas adheridas a este Código limitarán la utilización de datos proporcionados por los menores con la única finalidad de la promoción, venta y suministro de productos o servicios dirigidos a menores.

5. En ningún caso podrán cederse los datos relativos a menores sin el previo consentimiento de sus padres o tutores.

6. Las empresas adheridas a este Código deberán ofrecer a los padres o tutores información acerca de cómo proteger en línea (on-line) la privacidad de sus hijos o pupilos, así como facilitarles mecanismos para ejercer los derechos de acceso, rectificación, cancelación y determinación de la finalidad sobre los datos de aquéllos.

7. Las empresas adheridas a este Código también deberán apoyar cualquier esfuerzo que se realice por parte de otros organismos para ayudar a informar a los padres o tutores sobre cómo proteger en línea (online) la intimidad de sus hijos o pupilos, incluyendo información sobre herramientas de software y control de acceso para los padres, que impidan que los niños proporcionen su nombre, dirección y otros datos personales.

Título VI. Normas de aplicación del código

Articulo 29. Vinculación al Código

1. Las empresas que manifiesten su adhesión al presente Código Etico, por el solo hecho de su adhesión, se comprometen a respetar en sus actividades de publicidad y comercio electrónico las normas en él recogidas.

2. Las empresas que manifiesten su adhesión al presente Código Etico, por el solo hecho de su adhesión, se comprometen a plantear sus eventuales reclamaciones por la infracción de las normas del Código ante la Secretaría del presente sistema de autorregulación. Las empresas adheridas que desarrollen actividades publicitarias a través de medios electrónicos de comunicación a distancia se someten al sistema extrajudicial de resolución de controversias encarnado en el Jurado de la Publicidad. Por su parte, las empresas adheridas que realicen transacciones contractuales de comercio electrónico con consumidores se someten, para la resolución de las controversias que surjan por presunta infracción de las normas del presente Código relativas a la contratación con consumidores, y para el caso de que no hubieran podido ser resueltas por la mediación de AECE, al arbitraje de la Junta Arbitral Nacional de Consumo, que se constituye de acuerdo con lo establecido en el Real Decreto 535/1993, por el que se regula el Sistema Arbitral de Consumo. En consecuencia, las empresas que manifiesten su adhesión a este sistema de autorregulación se comprometen a acatar y cumplir escrupulosamente y con carácter inmediato el contenido de las resoluciones que el Jurado de la Publicidad o la Junta Arbitral Nacional de Consumo puedan emitir para la resolución de las reclamaciones contra concretas acciones publicitarias o transacciones contractuales realizadas a través de medios electrónicos de comunicación a distancia que les sean presentadas en relación a este Código.

3. Se hará publica la relación de empresas adheridas.

4. Las empresas adheridas al Código se comprometen a promover este sistema de autorregulación y a darlo a conocer y difundirlo tanto en los distintos sectores empresariales con los que estén relacionados como en la sociedad española en general —especialmente entre los usuarios de Internet y de otros medios electrónicos e interactivos—.

5. Las empresas adheridas a este Código y, por tanto, al sistema de autorregulación que éste establece, deberán informar de forma permanente, directa y de fácil acceso, y por medios electrónicos, sobre su adhesión a este Código, facilitando la posibilidad de consultarlo. Para el cumplimiento de dicho deber de información, y como muestra de su compromiso con las normas de este Código, las empresas adheridas podrán insertar en su web y en otras formas de comunicación (cartelería, etc.) el sello de confianza de este sistema de autorregulación, que deberá ser expuesto en lugar visible. El sello así insertado en la web de una empresa adherida deberá enlazar con la página web de este sistema de autorregulación, con el fin de ofrecer a los usuarios un fácil acceso a los contenidos del Código y a los listados de empresas adheridas, y deberá facilitarles la posibilidad de formular una queja o presentar una reclamación. La obtención y utilización del sello de confianza se regirá por lo dispuesto en el art. 32 del presente Código.

Artículo 30. Control del cumplimiento del Código

1. El control del cumplimiento de las normas del presente Código corresponderá a dos órganos extrajudiciales. De un lado, el Jurado de la Publicidad de Autocontrol, que se encargará de resolver las eventuales controversias relacionadas con las comunicaciones comerciales que sean presentadas por infracción de las normas contenidas en el presente Código. De otro, la Junta Arbitral Nacional de Consumo, que, de conformidad con el Real Decreto 636/1993, de 3 de mayo, por el que se regula el Sistema Arbitral de Consumo, se encargará de resolver las eventuales controversias relacionadas con la contratación electrónica con consumidores que sean presentadas por infracción de las normas contenidas en el presente Código, y que no hayan podido ser resueltas a través de la mediación de AECE en un plazo de siete días laborables desde su recepción. Ambos órganos se regirán en su actuación por los principios de independencia, transparencia, contradicción, eficacia, legalidad, libertad de elección y derecho de representación por parte del consumidor, establecidos en la Recomendación 98/257/CE. El Jurado de la Publicidad actuará de acuerdo con lo dispuesto en sus Reglamento y la actuación de la Junta Arbitral Nacional de Consumo se regirá por las normas que le resulten de aplicación.

2. En aras de una adecuada coordinación y eficacia en la tramitación y resolución de las controversias, la labor de ambos órganos contará con el apoyo de una Secretaría —dirigida conjuntamente por los Directores Generales de AECE y de Autocontrol de la Publicidad—, que se encargará de los aspectos de tramitación y procedimentales, y a la que se dirigirán las reclamaciones presentadas por pretendidas infracciones de las normas de este Código. La Secretaría se encargará asimismo de la elaboración de estadísticas y la adecuada promoción del sistema de autorregulación, así como de la asignación y administración cotidiana del sello de confianza, y de la gestión económica del sistema.

Artículo 31. Resolución extrajudicial de controversias

1. Se establecerán los mecanismos necesarios que permitan la presentación de reclamaciones on-line y la comunicación de las resoluciones también en línea a través de la página web de este sistema de autorregulación.

2. Todas las reclamaciones por la presunta infracción de las normas recogidas en el presente Código serán presentadas ante la Secretaría.

3. Además de las empresas que se hayan adherido al presente Código, podrán plantear reclamaciones, por infracción de las normas del presente Código, cualquier otra

empresa o asociación empresarial o profesional, así como consumidores individuales o asociaciones de consumidores, las Administraciones Públicas o, en definitiva, cualquier tercero con un interés legítimo que considere que se han vulnerado las normas de este Código.

4. Presentada una reclamación, la Secretaría dará traslado de la misma, según corresponda, a Autocontrol de la Publicidad o a la AECE, en función del contenido y la materia objeto de reclamación en cada caso (publicidad o transacción contractual).

5. La tramitación de las reclamaciones presentadas por presunta infracción de las normas de este Código en relación con la publicidad se desarrollará de acuerdo con lo establecido en el Reglamento del Jurado de la Publicidad, en el que, entre otras, y además de la intervención del Jurado, está prevista la posibilidad de la mediación de Autocontrol como vía para intentar resolver las reclamaciones.

6. Por su parte, las reclamaciones presentadas por presunta infracción de las normas de este Código en relación con transacciones contractuales con consumidores, serán, en todo caso, inmediatamente trasladadas a la AECE por la Secretaría. Una vez recibida la reclamación, AECE procederá a un intento de mediación, en un plazo de siete días laborables, con el fin de que las partes alcancen un acuerdo amistoso de la controversia.

   De no haberse alcanzado un acuerdo de mediación en el citado plazo de siete días desde la recepción, por AECE, de la reclamación presentada, la Secretaría dará traslado de la reclamación a la Junta Arbitral Nacional de Consumo, que la tramitará de conformidad con las normas que le resulten de aplicación.

7. Las resoluciones dictadas por el Jurado de la Publicidad o por la Junta Arbitral Nacional de Consumo serán inmediatamente comunicadas a las partes interesadas para su cumplimiento, y posteriormente hechas públicas a través de su inserción en la página web de este sistema de autorregulación, así como a través de las páginas web u otros medios de la AECE y Autocontrol de la Publicidad. Los casos que los órganos de gobierno de Autocontrol y/o la AECE consideren de especial gravedad, podrán ser activamente publicitados.

8. Los órganos de gobierno de las Asociaciones adheridas supervisarán e impondrán de manera eficaz le ejecución de las resoluciones firmes del Jurado de la Publicidad. En caso de incumplimiento de las resoluciones del Jurado y/o de la Junta Arbitral Nacional de Consumo, las empresas que hubieran mostrado formalmente su adhesión a este Código podrían ser privadas de la utilización del sello de confianza. Este hecho podrá ser hecho público por los medios que las Asociaciones adheridas estimen oportunos. Asimismo, en caso de grave incumplimiento de las resoluciones del Jurado o de reite-

rada infracción de las normas de este Código por parte de alguno de los miembros de las Asociaciones adheridas al sistema, éstas se reservan la facultad de expulsarles de sus respectivas asociaciones, lo que supondría asimismo la retirada inmediata del sello de confianza.

Articulo 32. Del Sello de Confianza: obtención, utilización, renovación y caducidad

1. Las empresas que se adhieran a éste Código de Conducta podrán identificarse con la exhibición en sus webs del Sello de Confianza de Comercio Electrónico y Publicidad Interactiva como distintivo de la adhesión al presente sistema de autorregulación. Al pulsar sobre el Sello de Confianza se proporcionará acceso a la información relativa al presente sistema de autorregulación del comercio electrónico y la publicidad interactiva, especialmente en lo atinente a las normas éticas plasmadas en este Código Ético y al funcionamiento de los mecanismos extrajudiciales de resolución de controversias encargados del control de su aplicación —permitiendo incluso la presentación de reclamaciones online—, así como al listado de las empresas y entidades adheridas a este sistema de autorregulación. Asimismo, las empresas adheridas podrán incluir el Sello de confianza en otros elementos de comunicación (cartelería, etc.).

2. Dado su objeto esencial, que es el de constituir una marca distintiva colectiva, el sello no podrá ser dispuesto ni, en todo caso, utilizado de tal forma que pueda ser considerado:
   — como una marca propia de la empresa usuaria,
   — o como una garantía de calidad de los productos o servicios ofrecidos.

3. La utilización del Sello de Confianza de manera fraudulenta constituye una infracción, debidamente sancionada por la legislación correspondiente. Entre otros, podría constituir una infracción de los derechos de exclusiva que recaigan sobre el sello, así como de la legislación publicitaria y de competencia desleal, que prohiben los actos de engaño.

4. Sólo podrán obtener y utilizar el Sello de Confianza las empresas que previamente se hayan adherido a este Código. Para la obtención del Sello de Confianza será necesario que la empresa adherida lo solicite a la Secretaría del sistema. Recibida la solicitud, la Secretaría enviará un acuse de recibo de la misma. La Secretaría solicitará a la empresa peticionaria la documentación necesaria que acredite la identidad de la empresa solicitante y además podrá solicitar cualquier aclaración o documentación complementaria necesaria para la obtención del Sello de Confianza así como proponer las medidas que crea necesarias para una mejor adecuación a lo establecido en el presente Código. Si, en tal supuesto, no se produce ninguna comunicación entre la empresa

solicitante y la Secretaría en los tres meses siguientes a las peticiones o propuestas de la Secretaría, se entenderá caducado el procedimiento de solicitud del sello, pudiendo la empresa pedir su reanudación en cualquier momento.

5. Una vez que la Secretaría del sistema acuerda el otorgamiento del Sello de Confianza la empresa deberá comprometerse formalmente al cumplimiento de sus condiciones de utilización. La Secretaría podrá, en todo momento, apreciar y controlar las condiciones de utilización del sello y tomar todas las medidas útiles en caso de utilización anómala. A estos efectos, las empresas adheridas se comprometen a aplicar sin demora y sin reserva las instrucciones de utilización que les sean comunicadas por la Secretaría.

6. Las empresas adheridas tendrán derecho a utilizar el Sello de Confianza durante el tiempo de su adhesión a este Código y sistema de autorregulación. Desde el momento en que una empresa adherida decidiese eventualmente finalizar su adhesión, automáticamente perdería su derecho a la utilización del Sello.

Título VII. Colaboración con las autoridades

Artículo 33.

Las empresas que desarrollen actividades de publicidad y comercio electrónico a través de medios electrónicos de comunicación a distancia tienen la obligación de colaborar con las autoridades competentes, y de poner en su conocimiento cualquier información relevante a la que haya tenido acceso, acerca de actividades presuntamente delictivas en la red (contenidos pornográficos referidos a menores, promoción o comercialización ilícita de medicamentos o drogas, proxenetismo, u otras que se encuentren tipificadas en el Código Penal español).

Disposición final

El presente Código, que deroga y sustituye al Código Ético de Protección de Datos Personales en Internet de la AECE, así como al Código Ético de Publicidad en Internet de AUTOCONTROL, estará sujeto a revisión periódica, con el fin de adaptarlo y mantenerlo actualizado en relación con los cambios que tengan lugar en la sociedad y el estado/desarrollo de las tecnologías. Cuando de esta revisión se siga la necesaria modificación del Código, ésta se realizará con la publicidad y audiencia necesarias.

Unió Catalana d'Hospitals
Associació d'Entitats Sanitàries i Socials

CODI TIPUS

Protegim les Vostres Dades Personals de Salut

CÓDIGO TIPO
DE LA UNIÓ CATALANA D'HOSPITALS

INTRODUCCIÓN

Con la entrada en vigor de la **Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal** (LOPD) se recondujo el desarrollo legislativo iniciado con la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD). Efectivamente esta última, desarrollo legislativo del Artículo 18.4 de la Constitución Española, pronto se vio superada por la legislación europea, y en concreto por la **Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa del 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 los mismos.**

La citada Directiva Europea, en su consideración segunda establece "*que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, de respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos.*"

Per tanto, más allá de lo que pretendía la LORTAD, es decir, ordenar el correcto uso de las nuevas tecnologías potenciando sus beneficios para la comunidad y limitando el riesgo que podía suponer para el honor y la intimidad de los ciudadanos, la LOPD desarrolla, en todo lo que concierne al tratamiento de datos personales, las garantías y protección de las libertades públicas y los derechos fundamentales de las persona físicas

y, especialmente, su honor y la intimidad personal y familiar. Es, por tanto, una regulación más global, superando las consideraciones técnicas al uso de las nuevas tecnologías, y centrándose en la utilización de datos, sea cual sea el dispositivo o mecanismo que los trate.

En este sentido, hay **dos elementos**, directamente resultantes del citado cuerpo legal, que explican la necesidad y conveniencia de la existencia de este documento.

En primer lugar, la diversa consideración que tienen los datos personales según su contenido. Nos referimos a la clasificación legal, en la que los **datos concernientes a la salud de las personas**, por su naturaleza indiscutible de datos sensibles, resultan especialmente protegidos, de tal manera que ello afecta a las condiciones que han de cumplirse para su obtención, tratamiento y seguridad.

En segundo lugar, la posibilidad de establecer **Códigos Tipo**[1], que no son otra cosa que acuerdos sectoriales, mediante los cuales los titulares y responsables del tratamiento de datos, a través de las organizaciones representativas de su sector de actividad, establecen normas de conducta que permiten la aplicación concreta de la Ley en su ámbito ordinario de actuación, considerando las especificidades de su actividad y como garantía para las personas afectadas por el tratamiento de sus datos.

Estos dos aspectos han conducido a la **Unió Catalana d'Hospitals, Associació d'Entitats Sanitàries i Socials**, a establecer en este documento los criterios y condiciones que han de permitir la construcción de un corpus de buenas practicas entre sus asociados, dirigidas directa-

[1] **LOPD art. 32 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 agrupan, 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. (…) **3.** Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional (…)

mente a garantizar, en el campo del tratamiento de datos concernientes a la salud de las personas afectadas, unos standard de referencia en estricto cumplimiento de la ley.

La **Unió Catalana d'Hospitals, Associació d'Entitats Sanitàries i Socials** es una asociación empresarial voluntaria de entidades prestadoras de asistencia sanitaria, sociosanitaria y social y de otras entidades proveedoras de bienes y servicios a aquellas, que tienen en común, con independencia de su forma jurídica, la función social de prestar servicios sanitarios y sociales a los ciudadanos. Su objeto principal es coordinar los esfuerzos de sus asociados para mejorar la función que las entidades prestadoras de asistencia sanitaria, sociosanitaria y social desarrollan al servicio de la comunidad y hacer esta función sostenible.

Iniciando sus actividades en el año 1975, se constituyó legalmente el año 1977 al amparo de la ley 19/1977 de 1 de abril, limitando su actuación a partir de 1985 al territorio de Cataluña, siendo registrada en el Ministerio de Trabajo y Seguridad Social y posteriormente en el Departamento de Trabajo de la Generalitat de Catalunya.

Así, el presente **CODIGO TIPO DE LA UNIÓ CATALANA D'HOSPITALS** nace para convertirse en un documento ágil y eficaz, referencia para el sector sanitario, socio-sanitario y social, y ceñido a los datos de carácter personal, especialmente los concernientes a la salud de las personas, tratados en los denominados genéricamente FICHEROS DE PACIENTES (Historia Clínica), por ser este el ámbito de especialización y diferenciación que presentan las organizaciones asociadas a la UNIÓ.

Su finalidad pues, será que los asociados al Código Tipo preserven de cualquier violación la privacidad de las personas físicas y garanticen su autodeterminación informativa. Por tanto se configura como una doble garantía: para los centros asociados en tanto a que su aplicación supondrá el cumplimiento de la normativa en los supuestos más concretos del sector, y para los usuarios que dispondrán de una referencia sectorial que asegurará la preservación de sus derechos.

CAPÍTULO I. Disposiciones generales.

Artículo 1. Ámbito subjetivo de aplicación.

1. El presente Código Tipo será de aplicación a:

    a. Todos los asociados a la Unió Catalana d'Hospitals, Associació d'Entitats Sanitàries i Socials (a partir de ahora UNIÓ) que manifiesten de forma expresa su adhesión al Código Tipo.

    b. Aquellas entidades no asociadas a la UNIÓ pero que, reuniendo las condiciones para poder ser asociado, manifiesten su voluntad de adhesión al Código Tipo.[2]

2. La UNIÓ dispondrá, en todo momento, de un listado de adheridos al Código Tipo, que remitirá con periodicidad anual a la Agencia de Protección de Datos, del mismo modo que también comunicará en cada momento las altas y bajas que se produzcan entre los adheridos, durante el mes inmediatamente siguiente en el cual estas se produzcan.

Artículo 2. Ámbito objetivo de aplicación.

El presente Código Tipo será de aplicación al tratamiento de datos de carácter personal contenidos en los ficheros de pacientes/historia clínica (a partir de ahora Ficheros de Pacientes), sea cual sea su soporte y modalidad de tratamiento, los cuales constituyen el elemento diferencial de los asociados a la UNIÓ y adheridos al presente Código Tipo. Por tanto sus disposiciones, supervisión y régimen disciplinario no serán de apli-

[2] Art. 6 de los estatutos de la UNIÓ: *Tipos de asociados. La Unió está constituida por asociados de dos tipos: Prestadores de asistencia: se trata de todo tipo de entidades prestadoras de asistencia sanitaria, sociosanitaria y social, tanto en régimen ambulatorio como domiciliario o de internamiento o asociaciones legalmente constituidas por estas entidades. Proveedores de bienes o servicios: se trata de entidades comerciales, industriales y/o profesionales proveedoras de bienes y servicios a las entidades proveedoras de asistencia.*
Artículo 1.2 de los estatutos de la UNIÓ: *Las entidades asociadas a la Unió tienen implantación en el ámbito territorial de Cataluña.*

cación al resto de datos contenidos en otros tipos de ficheros que los adheridos al Código Tipo traten.

Artículo 3. Condiciones de adhesión y periodo de adaptación.

1. La adhesión al Código Tipo en ningún caso modifica el régimen de obligaciones establecido por la legislación vigente, y en este sentido, para someterse a este documento será necesario cumplir las obligaciones legalmente establecidas, con especial consideración al registro de ficheros e implantación de los niveles de seguridad exigidos.[3]

2. En caso de aprobación de este Código Tipo por parte de la Agencia de Protección de Datos antes de que se hayan agotado los plazos establecidos para alguna de las obligaciones citadas, las entidades adheridas al Código Tipo deberán acreditar su cumplimiento en plazo para mantener dicha condición.

3. Una vez comunicada formalmente por la UNIÓ a las entidades adheridas la inscripción del Código Tipo por parte de la Agencia de Protección de Datos, las entidades adheridas dispondrán de un año de plazo para adaptar sus sistemas organizativos y sus documentos de seguridad a las indicaciones del Código Tipo, en los casos en que estas no estén contenidas en obligaciones legales cuyo cumplimiento ya deba producirse con carácter anterior.

[3] Actualmente los plazos pendientes se refieren a la implantación del Nivell Alto de seguridad (el aplicable a los datos de salud) el 26/06/2002, y la comunicación de ficheros no automatizados el 24/10/2007

CAPÍTULO II. Principios de la Protección de Datos.

SECCIÓN PRIMERA. Calidad de los datos de salud.

Artículo 4.

Les entidades adheridas al Código Tipo deben garantizar la calidad de los datos contenidos en los ficheros de pacientes, en los siguientes términos:

1. Los datos de los ficheros de pacientes sólo podrán recogerse y tratarse cuando sean adecuados, pertinentes y no excesivos en relación a la finalidad para la que se recogen; del mismo modo, esta finalidad deberá ser siempre determinada, explícita y legítima.

   Siendo la finalidad de la recogida de los datos de los ficheros de pacientes la prestación de la asistencia médico-sanitaria solicitada por el usuario, la recogida de los mismos se orientará a la determinación del motivo de dicha asistencia, a los antecedentes relevantes en relación a este, a la realización del proceso diagnóstico y al establecimiento del correspondiente tratamiento, así como aquellos otros datos que deben facilitar el abono de los gastos derivados de la asistencia.

2. Nunca podrán ser tratados con finalidades incompatibles a las que motivaron su recogida; no es incompatible la finalidad posterior de carácter científico y/o histórico, lo cual deberá realizarse de forma que los datos utilizados sean anónimos; en el supuesto de que sean utilizados los datos para la realización de ensayos clínicos o proyectos de investigación, los correspondientes protocolos deberán prever mecanismos que permitan la disociación de los mismos con respecto a la identidad de sus titulares. Se acompaña de anexo 1 modelo de cláusula a incorporar en los contratos entre el centro y el promotor del ensayo clínico.

3. Los datos serán exactos y puestos al día, respondiendo con veracidad a la situación actual; los centros adheridos al Código Tipo velarán por la cancelación de los datos incompletos o inexactos y su sustitución por los correctos;

4. Los datos de los ficheros de pacientes serán cancelados una vez dejen de ser necesarios y pertinentes para la finalidad para la que fueron recogidos; por lo que se refiere a las entidades adheridas al Código Tipo sometidas a la legislación de la Generalitat de Catalunya, y por imperativo del Artículo 12 de la *Ley 21/2000 de 29 de Diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica*, y en relación a los datos de salud que integran la Historia Clínica de la persona interesada, el criterio general de conservación es de 20 años desde la muerte del paciente, si bien se pueden cancelar datos no relevantes para la asistencia del interesado, transcurridos 10 años desde la última asistencia; se entiende como datos no relevantes, a los efectos mencionados en este apartado, aquellos que carezcan de utilidad futura para la realización de procesos diagnósticos o establecimiento de tratamientos. Finalmente, y en relación a lo que menciona la referida Ley catalana, si a criterio de los profesionales asistenciales hay razones que lo justifiquen a nivel preventivo, asistencial o epidemiológico, no hay límite temporal para conservar los datos relevantes.

5. Las entidades adheridas garantizan la seguridad de los datos, tanto en lo referente a su custodia y tratamiento, como en lo referente a permitir el acceso por el usuario afectado;

6. Las entidades adheridas al Código Tipo garantizan la no utilización de medios fraudulentos, desleales o ilícitos para la recogida de datos de salud.

SECCIÓN SEGUNDA. Derechos de los afectados.

Artículo 5. Consideración general.

Los derechos de los afectados, personas a las que pertenecen los datos de los ficheros de pacientes objeto de tratamiento por parte de las entidades adheridas al Código Tipo, son de obligado cumplimiento por parte de estas últimas y componen el núcleo de obligaciones central del presente documento.

Artículo 6. Derecho de información en la recogida de datos.

1. Los interesados a los que se recogen datos de salud, han de ser informados en ese momento de manera expresa, precisa e inequívoca de:

    a. la existencia de un fichero o tratamiento de datos de carácter personal al que se destinan los recogidos, con indicación de su denominación, que con carácter general será el de "fichero de pacientes";

    b. la finalidad de la recogida de estos datos, que habrá de consistir en la prestación de asistencia médico-sanitaria, ya sea en todas o cualquiera de las fases de la misma;

    c. los destinatarios de la información, que serán todos los departamentos en los que se organiza la entidad para poder llevar a cabo sus finalidades, así como las entidades públicas o privadas que por obligación legal o necesidad material, deban acceder a los datos a los efectos de la correcta prestación de la asistencia médico-sanitaria que constituye la finalidad del tratamiento de los datos;

    d. la posibilidad de ejercer los derechos de acceso, rectificación y cancelación, de acuerdo con las prescripciones de la LOPD, la

Instrucción 1/1998 de 19 de Enero de la Agencia de Protección de Datos, y del presente Código Tipo;

e. la identidad y dirección del responsable del tratamiento y en su caso, de su representante.

2. Tratándose de datos de salud y especialmente de las circunstancias en que son recogidos por las entidades adheridas al Código Tipo, no es exigible el cumplimiento de la obligación de informar sobre el carácter facultativo u obligatorio de las respuestas a las preguntas que sean planteadas así como de las consecuencias de la obtención de los datos o de la negativa a suministrarlos.[4]

3. Sin embargo, considerando las condiciones en que las entidades adheridas al Código Tipo realizan su actividad de prestación de servicios médico-sanitarios, podrán informar a las personas afectadas que la negativa a facilitar los datos solicitados puede impedir o bien la efectiva prestación de la asistencia sanitaria o el abono de su coste por parte del sistema sanitario público de salud u otro sistema privado con el que la persona afectada tenga contratada dicha prestación (seguros de salud, mutualidades, etc.)

4. El efectivo cumplimiento de la obligación de información a que hace referencia este Artículo se llevará a cabo por parte de las entidades adheridas al Código Tipo a través de los siguientes medios:

   a. Entrega a los usuarios de una hoja informativa con el contenido establecido en el anexo 2 de este CODIGO TIPO;
   b. Inserción en los folletos de información general del centro, en caso de haberlos, de una leyenda relativa a los extremos esenciales del documento contenido en el anexo 2 antes citado.

[4] LOPD, art. 5.3: No será necesaria la información a que se refieren las letras 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*) (…) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

c. Ubicación de paneles informativos en las áreas de admisiones y salas de espera de los centros con la leyenda que se establece en el anexo 3 de este CODIGO TIPO.

La acreditación del cumplimiento de la obligación de informar a la que se hace referencia en este Artículo será responsabilidad de las entidades adheridas, utilizando para ello cualquier medio jurídicamente hábil a tal fin, si bien se entenderá acreditado dicho cumplimiento mediante la custodia de un ejemplar del documento de información firmado por el usuario.

Artículo 7. Consentimiento de la persona afectada.

1. Con carácter general la recolección de datos supone la necesidad de obtener el consentimiento inequívoco del afectado. La LOPD considera más concretamente que el consentimiento debe consistir en una manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el afectado consiente el tratamiento de sus datos personales.

2. Con todo, los datos que integran el fichero de pacientes disponen de un régimen especial, determinado por la autorización a las instituciones, centros sanitarios, públicos o privados, y a los profesionales correspondientes, al tratamiento de los datos concernientes a la salud de las personas que a ellos acudan o hayan de ser tratadas en los citados centros, de acuerdo con lo que dispone la legislación estatal o autonómica sobre sanidad;[5]

Artículo 8. Obligación de garantizar la seguridad de los datos.

1. Su objetivo consiste en evitar la alteración, perdida, tratamiento o acceso no autorizado a los datos de carácter personal.

[5] LOPD art. 8

2. La seguridad se garantizará por parte de las entidades adheridas al Código Tipo mediante la adopción de las medidas de índole técnica y/o organizativa necesarias.

3. La Disposición Transitoria Tercera de la LOPD mantiene en vigor la regulación de desarrollo de la anterior LORTAD[6], de aplicación a los ficheros de pacientes automatizados. Por lo que se refiere a los ficheros de pacientes en soporte físico no automatizado o papel, si bien no es de aplicación la referida normativa, las entidades adheridas al Código Tipo aplicaran las medidas establecidas en el anexo 4 de este documento.

4. La aplicación de la normativa antes citada lleva en primer lugar a considerar que los datos contenidos en los ficheros de pacientes requieren el nivel alto, en el caso de tratarse de ficheros automatizados (es decir, el nivel máximo que implica la adopción también de las medidas contenidas en los niveles inferiores). En segundo lugar, comporta la obligación de que las entidades adheridas al Código Tipo dispongan de un documento de seguridad para la implantación en su organización de las medidas previstas en la normativa de aplicación.

5. El Comité Directivo del Código Tipo velará por la adecuación de los documentos de seguridad de las entidades adheridas a las prescripciones legales y reglamentarias y a las prescripciones del propio Código Tipo.

6. En lo concerniente a los datos contenidos en los ficheros automatizados de pacientes, la implantación del nivel Alto supone que el documento de seguridad debe contemplar los siguientes ítems, que aquí se mencionan enunciativamente pero que aparecen desarrollados en la norma reglamentaria antes citada:

   a. Ámbito de aplicación con relación de los recursos protegidos.

[6] Real Decreto 994/1999, reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

b. Medidas de verificación de las normas del propio documento de seguridad.

c. Funciones y obligaciones del personal. Establecimiento e identificación de la figura del responsable de seguridad de los ficheros.

d. Accesos del personal autorizado: identificación, autenticación y registro de accesos; control de acceso físico.

e. Estructura de los ficheros y descripción de los sistemas de información.

f. Procedimientos de notificación, gestión y respuesta ante las incidencias; registro de incidencias.

g. Procedimientos de realización de copias de seguridad y recuperación de datos; ubicación de las copias de seguridad.

h. Gestión de soportes informáticos; medidas para supuestos de inutilización y reutilización de algún soporte, impidiendo la recuperación de datos en el primer caso; registro de entrada y salida de soportes; distribución física de soportes.

i. Cifrado de los datos que se transmitan.

j. Auditoria.

7. En lo concerniente a los datos contenidos el los ficheros de pacientes en soporte físico no automatizado o papel, la adaptación de los requisitos del nivel alto exigidos para los ficheros automatizados, se llevará a cabo por las entidades adheridas al Código Tipo mediante la incorporación a los documentos de seguridad de los criterios e indicaciones contenidos en el anexo 4 de esta documento

Artículo 9. Obligación de Secreto.

1. La obligación o deber de secreto profesional en relación a los datos personales contenidos en los ficheros de pacientes es inherente a la condición de los profesionales vinculados al proceso asistencial, impuesto por sus propias normas deontológicas, al margen de las disposiciones de la legislación sanitaria y, en último término, sancionado por el derecho penal. A pesar de ello, las entidades adheridas al Código Tipo velarán por recordar a sus profesionales el cumplimiento de este deber.

2. Por lo que se refiere al personal no vinculado al proceso asistencial pero con acceso a los datos contenidos en los ficheros de pacientes, deberá obtenerse, por parte de la entidad con la que ostente contrato de trabajo, la firma de un documento de compromiso, relativo al cumplimiento del deber de secreto, que contendrá las advertencias pertinentes en relación a las consecuencias que implicaría su incumplimiento, tanto desde una perspectiva disciplinaria laboral, como desde la perspectiva del derecho de repetición que la entidad ostenta ante posibles sanciones o indemnizaciones económicas a las que tenga que hacer frente. Como anexo 5 a este documento se acompaña modelo de documento de confidencialidad en los términos aquí previstos.

Artículo 10. Cesión de los datos.

1. El criterio general que establece la norma legal hace referencia a dos aspectos básicos en el campo de la cesión de datos de carácter personal:

    a. Únicamente se podrá llevar a cabo para el cumplimiento de las finalidades directamente relacionadas con las funciones legítimas de quien cede y de quien recibe la cesión, y

b. Será necesario el consentimiento de la persona afectada, que habrá de recibir información completa respecto a la cesión que se efectúa.

2. También con carácter general, no requieren el consentimiento mencionado las urgencias en lo referente a los datos de salud, así como las determinaciones de la legislación sanitaria en relación a los estudios epidemiológicos (por ejemplo: enfermedades de declaración obligatoria).

3. El pago de los servicios sanitarios, socio-sanitarios y sociales viene determinado en la practica totalidad de los casos, por lo que se refiere a la actividad realizada por las entidades adheridas al Código Tipo, por una relación jurídica entre el usuario y el financiador de los servicios (sistema público de salud o entidades privadas de salud, mutualidades, etc.), lo cual implica una necesaria cesión de datos de los ficheros de pacientes a dichas entidades. Dicha cesión se realizará solo en relación a los datos necesarios para poder establecer los criterios de pago adecuados, y deberá contar con el consentimiento del usuario, al cual se le advertirá de que la negativa a prestar dicho consentimiento implica el nacimiento de la obligación de pago directo y a su cargo, de los costes de la asistencia que le sea prestada.

4. Por todo ello, en el documento de información referido en el artículo 6 de este Código Tipo se hará referencia al consentimiento para dicha cesión de datos en los términos aquí establecidos y con las consideraciones contenidas en el párrafo anterior.

Artículo 11. Acceso a los datos por terceros.

1. Vista la complejidad cada día creciente de la asistencia sanitaria, socio-sanitaria y social, es un hecho incontestable que rara vez esta se puede llevar a cabo tan solo con los dispositivos y mecanismos de que dispone la entidad que realiza el tratamiento médico-sanitario del enfermo. El uso de servicios intermedios sanitarios externos (trans-

porte sanitario, diagnóstico por la imagen, laboratorio, etc.) y la realización de técnicas diagnosticas y terapéuticas especializadas, entre otras, son elementos que justifican el acceso a los datos contenidos en los ficheros de pacientes.

2. En estos casos no se está ante una cesión de datos, y por tanto no será necesario el consentimiento, si bien el documento de información referido en el artículo 6 de este Código Tipo deberá hacer mención genérica a esta transmisión de datos en el ámbito de las necesidades materiales de la correcta prestación del servicio.

3. También será requisito indispensable que entre la entidad adherida al Código Tipo y la entidad encargada del tratamiento de los datos en los casos a que se refiere este artículo, se establezca por escrito contrato o acuerdo donde determinen claramente que los datos serán tratados de acuerdo a las instrucciones facilitadas por el responsable del tratamiento de la entidad adherida al Código Tipo y que el encargado del tratamiento no las aplicará a otra finalidad diferente, ni las comunicará a terceros. En el mismo acuerdo se obligará el encargado del tratamiento a implementar las medidas de seguridad pertinentes atendida la naturaleza de los datos de los ficheros de pacientes y se comprometerá a su devolución o destrucción una vez finalizada la prestación contractual o cumplida la obligación legal de conservarlas, en caso de existir. Como anexo 6 a este Código Tipo se acompaña modelo de cláusula contractual cuyo contenido preserva las obligaciones referidas en este artículo.

4. También se establecerán las mismas condiciones con las entidades o empresas a las que las entidades adheridas al Código Tipo puedan contratar, en su caso, la gestión documental y el almacenamiento de los ficheros de pacientes.

SECCIÓN TERCERA. Garantías para los afectados.

Artículo 12. Oposición, acceso, rectificación y cancelación.

1. Los derechos de las personas afectada merecen una especial protección; en este sentido, las condiciones de su ejercicio se encuentran reguladas en la Instrucción 1/1998 de 19 de Enero dictada por la Agencia de Protección de Datos, vigente y de aplicación, a pesar de que su redactado se realizó en desarrollo de la LORTAD, y por tanto, debe entenderse extendido también a los ficheros no automatizados, en la medida de lo posible.

2. Los derechos de oposición, acceso, rectificación, y cancelación se caracterizan por los siguientes rasgos:

   a. son personalísimos, y por tanto los ejercerá el afectado o su representante legal.

   b. son independientes, por tanto el ejercicio de ninguno de ellos ha de ser requisito previo para el ejercicio de otro.

   c. se ejercitan por escrito, ante el responsable del fichero, en el que ha de constar:

      i) nombre y apellidos del interesado
      ii) copia del DNI del interesado o del representante legal; en el segundo caso, también el documento que acredite la representación.
      iii) petición concreta de la solicitud.
      iv) domicilio para notificaciones, fecha y firma.
      v) documentos acreditativos de lo solicitado, en su caso.
      vi) las entidades adheridas al Código Tipo facilitarán los medios para presentar estos escritos, entregando al interesado una copia con constancia de su recepción. Como anexos 7, 8 y 9 a este Código Tipo se acompañan modelos de

instancia normalizada para ejercer los derechos de acceso, rectificación y cancelación.

d. El responsable del fichero contestará las solicitudes, aunque en el fichero no existan datos personales del solicitante. Previamente, deberá pedir al interesado que corrija los posibles defectos de la solicitud, en caso de que los tuviera.

e. Para garantizar el ejercicio de estos derechos, las entidades adheridas al Código Tipo se aseguraran de que toda persona de su organización que intervenga en el tratamiento de datos personales conozca el procedimiento para poder informar a las personas afectadas.

3. El derecho de acceso implica que toda persona puede solicitar y obtener información de sus datos de carácter personal incluidos en su fichero de pacientes en las entidades adheridas al Código Tipo.

4. La persona afectada podrá hacer efectivo este derecho, consultando sus datos (siempre que la configuración de los mismos y de los sistemas de tratamiento lo permitan) a través de:

   a. visualización por pantalla,
   b. escrito, copia o fotocopia remitida por correo,
   c. telefax,
   d. cualquier otro sistema ofrecido por la entidad adherida al Código Tipo.

   En los supuestos en que la obtención de copia suponga un coste elevado por motivos técnicos justificados, la entidad adherida deberá advertir al afectado de este extremo y facilitarle alternativas para que se efectúe el acceso a sus datos.

5. La respuesta a la petición de acceso deberá responderse en el plazo de un mes; si no es así, la persona afectada queda facultada para interponer las correspondientes reclamaciones administrativas.

6. En caso de resolver favorablemente la petición, su ejercicio deberá llevarse a cabo en los 10 días siguientes a la comunicación favorable.

7. Se podrá denegar si el afectado ha ejercido este derecho de acceso en los 12 meses anteriores a la solicitud y no justifica causa legítima para el nuevo acceso, o en el caso de solicitarlo una persona distinta de la afectada.

8. La consulta deberá permitir una información legible e inteligible; afectara a los datos personales y a los datos elaborados a partir de ellos, al origen de los datos, las persona o entidades a quien se hayan cedido y especificación concreta de finalidades y usos por los que los datos fueron guardados. Tratándose de carácter personal contenidos en los ficheros de pacientes, y en relación a la entidades adheridas sometidas a la legislación de la Generalitat de Catalunya, de acuerdo con lo que establece el Artículo 13 de la *Ley 21/2000 de 29 de Diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica,* los profesionales que han intervenido en la elaboración de aquellos podrán invocar la reserva de sus observaciones, apreciaciones y anotaciones subjetivas, y por tanto estas quedaran fuera del derecho de acceso aquí regulado.

9. Referente a los derechos de rectificación y cancelación, se podrán ejercitar en caso de que los datos sean inexactos o incompletos, inadecuados o excesivos.

10. La efectividad de estos derechos se llevará a cabo por el responsable del fichero en los 5 días siguientes a la recepción de la solicitud, termino en el cual también lo notificará a les entidades o personas a las que se hubieran cedido los datos, para procedan de igual forma.

11. Para poder proceder a la rectificación, la solicitud deberá indicar el dato incorrecto y su corrección, acompañando la documentación jus-

tificativa, a excepción de que la corrección afecte exclusivamente a un consentimiento de la persona afectada.

12. Para poder proceder a la cancelación, deberá indicarse la revocación del consentimiento cuando sea revocable, o la cualidad de inexacto o erróneo del dato, acompañando la justificación pertinente. Los datos de los ficheros de pacientes no podrán ser objeto de cancelación, dado el deber de conservación a que hace referencia la *Ley 21/2000 de 29 de Diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica* para los centros sometidos a ella, tal como se menciona en el Artículo 4.4) de este Código Tipo.

13. Tampoco podrán ser objeto de cancelación los datos, si la cancelación causa un perjuicio a los intereses legítimos de la persona afectada o de terceros, o por la existencia de otra obligación de conservación, más allá de la citada en el apartado anterior.

14. Si se considera que la cancelación o rectificación no procede, se comunicará a la persona afectada, en un plazo de 5 días; si no se realiza esta comunicación, quedan abiertas las vías para ejercitar, por parte de la persona afectada, las reclamaciones administrativas pertinentes.

15. En el caso de proceder la cancelación, esta deberá hacerse mediante la eliminación física de los datos; si no fuera posible tanto por razones técnicas como de procedimiento, los datos se bloquearan impidiendo ulteriores procesos y utilizaciones.

CAPÍTULO III. Organización del Código Tipo.

Artículo 13. Comité Directivo.

1. El presente Código Tipo dispondrá de un Comité Directivo, compuesto por 9 personas designadas por la Junta Directiva de la UNIÓ. Actuará como Presidente del Comité el Presidente de la UNIÓ. La condición de miembro del Comité Directivo no está sometida a una duración temporal concreta, siendo revocable en todo momento el nombramiento por la Junta Directiva de la UNIÓ. El Comité Directivo contará con un asesor jurídico que podrá ser miembro o no.

2. El Comité Directivo se reunirá tantas veces como lo considere necesario su Presidente, y en cualquier caso una vez cada semestre.

3. Las funciones del Comité Directivo serán las siguientes:

    a. Monitorizar el desarrollo del Código Tipo, evaluar la evolución de su aplicación, y en su caso, elaborar las propuestas de modificación que deberán ser elevadas a la Asamblea de la UNIÓ para su aprobación, previo al trámite de autorización administrativa por parte de la Agencia de Protección de Datos.

    b. Representar al Código Tipo ante la Agencia de Protección de Datos, manteniéndola informada, en todo momento, de la marcha de su aplicación, y responsabilizándose de cumplir todas las obligaciones que como titular del Código Tipo la legislación impone ante la citada Agencia.

    c. Mantener al día la relación de entidades adheridas al Código Tipo y transmitir la información al respecto a la Agencia de Protección de Datos, de acuerdo con lo que establece el Artículo 1.2 de este documento.

    d. Resolver sobre las peticiones de alta o baja de adhesión al Código Tipo que se le formulen.

e. Dictar las instrucciones o circulares pertinentes sobre interpretación de las normas del Código Tipo, previa consulta con la Agencia de Protección de Datos.

f. Resolver los expedientes disciplinarios que se instruyan al amparo de lo que se establece en este Código Tipo.

g. Organizar un sistema de asesoramiento y de auditoria en relación a la aplicación del Código Tipo. Determinar, en su caso, los criterios retributivos que se puedan establecer por servicios a los asociados al Código Tipo.

h. Consultar y llegar a acuerdos de colaboración con entidades e instituciones representantes de colectivos de usuarios de la sanidad, a efectos de obtener el consenso en la aplicación del Código Tipo.

i. Cualquier otra que sea necesaria y pertinente para el correcto desarrollo del Código Tipo.

4. El Comité Directivo podrá nombrar un Secretario, que puede ser uno de sus miembros o una persona externa. En este último caso, participará en las reuniones, con voz pero sin voto.

5. De las reuniones del Comité Directivo se levantará acta que será firmada por el Presidente y el Secretario, y se habilitará un libro de actas donde estas quedarán registradas.

6. El Comité Directivo podrá establecer y nombrar un grupo de trabajo que llevará a cabo las funciones ordinarias de monitorización del Código Tipo, organización de los servicios de asesoramiento y auditorias a las entidades adheridas, y que instruirá los expedientes disciplinarios puestos en marcha a tenor de las disposiciones de este documento.

Artículo 14. Modelos documentales.

El Comité Directivo del Código Tipo podrá elaborar modelos de los documentos en aplicación de las disposiciones legales sobre protección de datos y de las de este Código Tipo, que deberán servir de referencia a las entidades adheridas para su aplicación. En cualquier caso, las entidades adheridas podrán elaborar sus propios documentos, adecuados a sus especificidades organizativas, pero en ningún caso podrán contradecir los modelos standard elaborados por el Código Tipo.

Artículo 15. Auditorias.

1. El Comité Directivo del Código Tipo organizará un servicio de auditoria externa a disposición de las entidades adheridas que contemplará la corrección de la aplicación de la legislación y del presente Código Tipo, y dará cumplimiento a la obligación de llevar a cabo la auditoria bianual especificada en la ley, o en un plazo inferior si se estima conveniente.

2. Asimismo también con carácter bianual, pero en años alternos a las auditorias previstas por la ley, las entidades adheridas deberán someterse a un control de seguimiento del Código Tipo, durante el cual se acreditará el cumplimiento de la obligación legal de someterse a auditoria, así como el cumplimiento de las prescripciones de valor añadido que incorpora el presente Código Tipo.

Artículo 16. Asesoramiento.

El Comité Directivo del Código Tipo habilitará los mecanismos de asesoramiento necesarios para las entidades adheridas, que les permitan la resolución de dudas y consultas puntuales. También podrá establecer instrumentos para asesoramientos con más profundidad e intervenciones correctoras.

Asimismo podrán establecerse mecanismos de información y consulta para los usuarios y ciudadanos en general a través de un "microsite" en la web de la UNIÓ.

Artículo 17. Publicidad y difusión.

1. La UNIÓ diseñará un logotipo del Código Tipo que servirá de símbolo distintivo de las entidades adheridas. Este logotipo, que permitirá la indicación del código o registro de la entidad adherida, deberá estar presente en las áreas de admisiones y salas de espera de los centros adheridos. También lo deberán insertar en sus páginas web en caso de disponer de ellas.

2. Toda comunicación de texto que las entidades adheridas dirijan a sus usuarios deberá igualmente contener el citado logotipo.

3. Las entidades adheridas deberán tener ejemplares del Código Tipo a disposición de sus usuarios para su consulta, anunciándolo debidamente en las áreas de admisiones y salas de espera. También deberán de articular los mecanismos por los cuales podrán entregar copia en caso que les sea solicitada, sin que ello signifique ningún coste para el usuario.

4. El texto del Código Tipo estará presente y a disposición para consultar en la página web de la UNIÓ, por lo cual podrá también ser referenciado por las entidades adheridas a los usuarios, así como instalar un link en su propia página web.

CAPÍTULO IV. Procedimiento de resolución de conflictos.

Artículo. 18. Consideración general.

Lo aquí establecido lo es sin perjuicio de la potestad sancionadora que la LOPD y disposiciones concordantes y de desarrollo atribuyen a la Agencia de Protección de Datos y a la facultad de las personas afectadas de dirigirse a los tribunales ordinarios en reclamación de las indemnizaciones que estimen oportunas por los daños y perjuicios que les hayan irrogado los incumplimientos de la Legislación y del Código Tipo por parte de las entidades adheridas.

Artículo 19. Derecho de queja.

1. Toda persona que considere que una entidad adherida actúa en relación a sus datos personales contenidos en el fichero de pacientes contraviniendo lo que dispone la ley o este Código Tipo, podrá dirigirse al responsable del fichero, identificándose de manera suficiente y exponiendo por escrito el contenido de la queja. Por anexo 10 a este Código Tipo se acompaña modelo normalizado de escrito de queja.

2. El derecho de queja deberá de ejercitarse en el plazo de un mes desde que haya tenido conocimiento de la pretendida infracción.

3. Las entidades adheridas al Código Tipo habilitaran los mecanismos necesarios para que la persona afectada tenga constancia documental de la fecha de presentación y recepción del escrito de queja.

4. En el caso de que la queja sea procedente, la entidad adherida al Código Tipo deberá de modificar el comportamiento objeto de la citada queja y notificarlo a la persona interesada, en el plazo máximo de un mes desde su presentación.

5. En el caso de que la entidad adherida al Código Tipo considere que no ha lugar a la queja formulada, deberá comunicarlo también en el plazo máximo de un mes a la persona afectada.

Artículo 20. Régimen disciplinario.

1. En caso de que la entidad adherida al Código Tipo no estime procedente el objeto de la queja o no la responda en el plazo establecido, la persona afectada podrá dirigirse al Comité Directivo del Código Tipo, mediante escrito en el que consten sus datos de identificación y el objeto de la queja, indicando y acreditando haber formulado queja ante la entidad adherida. Por anexo 11 a este Código Tipo se acompaña modelo normalizado de escrito de queja ante el Comité Directivo del Código Tipo.

2. El Comité Directivo del Código Tipo ordenará la incoación de un expediente disciplinario, nombrando instructor, comunicándose ambos extremos a la persona afectada y a la entidad adherida al Código Tipo.

3. El instructor del expediente oirá a las partes, que podrán actuar acompañadas de un asesor y aportar la documentación que crean oportuna en defensa de sus intereses.

4. En el plazo de un mes desde la fecha de incoación del expediente, el instructor nombrado deberá elevar una propuesta de resolución al Comité Directivo que la resolverá en la próxima reunión.

5. En caso de que la actuación de la entidad adherida al Código Tipo haya contravenido las disposiciones legales o el Código Tipo, con independencia de la obligación de adoptar de manera inmediata las medidas correctoras, será objeto de una amonestación por escrito por parte del Comité Directivo.

6. La resolución acordada no será recurrible y se comunicará a la persona interesada y a la entidad adherida.

7. Así mismo el Comité Directivo del Código Tipo podrá adoptar resoluciones sancionadoras contra cualquier entidad adherida ya sea a partir de un expediente de queja formulado por un usuario, ya sea a partir de la propia función de control de seguimiento del Código Tipo que tiene encomendada.

8. Las resoluciones sancionadoras consistirán en:

   a. Amonestación por escrito.

   b. Baja obligatoria del Código Tipo durante un período de hasta 2 años, en el caso de que recaigan tres o más amonestaciones escritas en el periodo de un año natural.

   c. Baja definitiva del Código Tipo en el caso de que la entidad adherida incumpla reiteradamente las prescripciones del Código Tipo y asimismo no implemente las medidas correctoras que le sean sugeridas por el Comité Directivo.

9. Las sanciones disciplinarias adoptadas por el Comité Directivo estarán a disposición de la Agencia de Protección de Datos que podrá solicitar copia certificada de la resolución.

CAPÍTULO V. Disposiciones finales.

Primera.

El presente Código Tipo solo podrá ser objeto de modificación y extinción, por acuerdo de la asamblea de asociados de la UNIÓ, a propuesta del Comité Directivo del Código Tipo, y previo informe favorable, en caso de modificación, de la Agencia de Protección de Datos.

Segunda.

Junto con la petición de aprobación del Código Tipo, la UNIÓ remitirá a la Agencia de Protección de Datos la relación de miembros del Comité Directivo del Código Tipo; todas las modificaciones en la composición del Comité Directivo del Código Tipo serán comunicadas a la Agencia de Protección de Datos.

ANEXO 1

El promotor del presente ensayo clínico garantiza que el protocolo del mismo establece los mecanismos que permiten la disociación de los datos de carácter personal contenidos en el fichero de pacientes en relación a los sujetos que participan en el ensayo. En cualquier caso se obliga el promotor a cumplir y hacer cumplir las prescripciones establecidas en la Ley Orgànica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal en todo lo que haga referencia a los datos de dicha índole que sean utilizados en el desarrollo del ensayo.

ANEXO 2

En virtud de lo dispuesto en los artículos 4,5 y 6 de la Ley Orgánica 15/1999 de 13 de diciembre, ***……centro……*** pone en su conocimiento que dispone de un fichero con datos de carácter personal denominado ***……nombre del fichero o tratamiento……*** de ***……centro……***

La finalidad de su creación es el tratamiento médico-sanitario a los usuarios de nuestro centro, en su totalidad o parte del mismo.

Los destinatarios de la información son todos los departamentos en los que se organiza ***……centro……*** así como los estamentos oficiales públicos y privados que por obligación legal o necesidad material hayan de acceder a los datos a los efectos de la correcta prestación de la asistencia médico-sanitaria que constituye la finalidad del tratamiento de estos datos.

En todo caso, usted tiene derecho a ejercitar los derechos de oposición, acceso, rectificación y cancelación en el ámbito reconocido por la Ley Orgánica 15/1.999 de 13 de diciembre, así como en el Código Tipo de la Unió Catalana d'Hospitals al que este centro está adherido.

El responsable del fichero es ***……responsable del fichero y/o tratamiento……***. Para ejercitar los derechos arriba mencionados, y para cualquier aclaración, puede dirigirse por escrito mediante instancia dirigida al Director de ***……centro……*** en su domicilio sito en ***……domicilio……***

Asimismo y por la presente consiento expresamente y autorizo a ***……centro……*** para que ceda los datos que sean estrictamente necesarios para que por la entidad con la que tengo concertada la prestación de los servicios médico-sanitarios que solicito pueda proceder al pago de los costes de los mismos, aceptando que en el caso de revocar el presente consentimiento ello significará que me corresponderá a mi personalmente hacerme cargo del pago de los mismos.

……el interesado……

(firma)

ANEXO 3

LEY ORGÁNICA 15/1999, de 13 de diciembre,
sobre PROTECCION DE DATOS DE CARÁCTER PERSONAL

A. Este centro, entidad adherida al CODIGO TIPO DE LA UNIÓ CATALANA D'HOSPITALS con el número de registro ……, garantiza la seguridad de sus datos de carácter personal contenidos en el Fichero de Pacientes.

B. Dichos datos se destinarán única y exclusivamente a la finalidad de procurar la atención médico-sanitaria que nuestros usuarios requieren.

C. Todo usuario podrá ejercer los derechos de oposición, acceso, rectificación y cancelación de sus datos de carácter personal, de acuerdo con las leyes.

D. Para cualquier información en relación al ejercicio de sus derechos, los usuarios pueden dirigirse a ……, responsable de tratamiento de sus datos, en ……

ANEXO 4

CRITERIOS DE SEGURIDAD DE LA HISTÒRIA CLINICA EN SOPORTE FÍSICO NO AUTOMATIZADO O PAPEL

Los procedimientos a aplicar en relación al uso y custodia de la historia clínica deben garantizar plenamente el derecho del paciente a su intimidad personal y el deber de guardar secreto para quien, en virtud de sus competencias, tenga acceso a la historia clínica.

Con este objetivo general, se establecen las siguientes pautas de conducta en relación al uso y custodia de la Historia Clínica (HC):

1. Cada HC es única y tendrá un número único para cada paciente de la entidad adherida y en ella se recogerá toda la información integrada y acumulativa relativa al curso clínico del paciente.

2. En cada una de las HC deberá incorporarse la constancia de que se ha facilitado al paciente la hoja de información en relación a sus derechos sobre los datos personales contenidos en su HC, con el correspondiente acuse de recibo.

3. Las HC estarán custodiadas en un archivo único. Sin embargo, puede preverse la existencia de un archivo pasivo, físicamente diferenciado del archivo activo, en el cual podrán ubicarse las HC correspondientes a pacientes sin contacto con el centro durante un determinado periodo.

4. En aquellos casos en que el archivo de HC pasivas se encuentre fuera de las dependencias del centro deberán garantizarse unas medidas de seguridad idénticas a las que existieran en el propio centro.

5. En aquellos casos en que el archivo de HC pasivas se encuentre fuera de las dependencias del centro y gestionado por una empresa externa, deberá ser formalizado por escrito un contrato que regule expresamente el deber de confidencialidad del depositario de las HC así como también el resto de obligaciones como encargado del tratamiento.

6. Cada centro deberá establecer un responsable de archivo de HC, que deberá velar por el adecuado cumplimiento de los sistemas de archivo, control e información, que deberán ser adecuados a las características y dimensiones del centro.

7. El acceso al archivo de HC deberá encontrarse limitado al horario en que el personal de archivo pueda ejercer los controles previstos. Fuera de este horario, el acceso al archivo estará restringido y controlado. Cualquier acceso al archivo fuera del horario habitual, deberá ser anotado en un registro creado al efecto.

8. El archivo de HC contará con medidas de seguridad física apropiadas.

9. En cualquier entrega interna de una HC, debe quedar constancia de la persona que efectúa la petición, o del motivo que justifica el flujo de las HC por razones or-

ganizativas y de programación de actos clínicos que requieren el acceso a las mismas.

10. Las salidas de HC del archivo deberán anotarse en un libro registro, con la información suficiente para permitir su seguimiento. En el mismo libro registro deberá anotarse también la fecha de devolución de la HC

11. Las solicitudes de HC de pacientes que en el momento de la solicitud no estén siguiendo un curso clínico, deberán ser debidamente justificadas.

12. La devolución de las HC al archivo debe realizarse inmediatamente después de la circunstancia que motivo su petición.

13. En ningún caso la HC puede salir de las dependencias del centro durante el periodo en que se ha hecho una petición por motivos asistenciales, docentes o de investigación.

14. Durante el periodo en que la HC se encuentra fuera del archivo central, deberán establecerse unas medidas de seguridad físicas mínimas que permitan restringir el acceso de personas no autorizadas.

15. Si se produjera una petición de HC por personal facultativo ajeno al centro por motivos docentes o de investigación, diferentes del propio proceso asistencial, deberá recabarse previa autorización expresa del paciente, siempre que los datos de la HC no pueda ser entregada en modo disociado.

16. Deberán establecerse los circuitos oportunos que permitan al paciente, o su representante legal, ejercer el derecho de acceso a su propia HC. La petición de acceso a la HC deberá ser realizada por escrito y de manera que se acredite la identidad del solicitante.

17. El paciente tendrá en cualquier caso acceso a la información que conste en su HC relativa a informes de alta, informes de urgencias, informes de pruebas diagnósticas y exploraciones complementarias, analíticas y similares. Siempre que el profesional no invoque reserva al respecto, podrán entregarse también hojas de curso clínico y documentos similares que contengan apreciaciones subjetivas de los profesionales que han participado en el tratamiento del paciente.

18. En ningún caso se entregará documentación original de la HC, debiendo informarse de manera previa al solicitante, del coste que pudiera suponer la obtención de copias de la misma en los casos en que la obtención de la copia tenga un coste extraordinario por el soporte de la misma, ofreciendo si es posible, alternativas al respecto.

19. En aquellos casos en que se reciba una solicitud o requerimiento de información clínica procedente de la Administración de Justicia, solicitando la remisión de una HC se recabará la autorización del responsable del centro y únicamente se enviará copia de la documentación en ella contenida. La remisión de la HC se acompañará de un escrito del responsable del centro en el cual se manifieste el deber de confidencialidad de los datos clínicos.

20. Las HC únicamente serán canceladas una vez transcurrido el plazo previsto por la normativa vigente (Ley 21/2000 de la Generalitat de Cataluña).

21. Los criterios establecidos en este anexo serán incorporados al documento de seguridad de cada entidad adherida, con excepción de aquellos supuestos que, debidamente justificados, no puedan ser implantados en la entidad. En estos casos deberán establecerse medidas o criterios alternativos adecuados a las circunstancias de la entidad afectada.

22. En el supuesto que, una vez cumplido el plazo previsto por la LOPD para el registro de ficheros no automatizados, el Código Tipo se adaptará a las disposiciones reglamentarias que se dicten en su caso para este tipo de ficheros; de no producirse dicho desarrollo reglamentario y de existir determinadas HC para las que no haya sido posible facilitar a su titular la hoja de información prevista en el criterio 2, el Comité Directivo del Código Tipo establecerá formulas y mecanismos oportunos al respecto para garantizar los derechos de los usuarios afectados.

ANEXO 5

De acuerdo con lo establecido en el artículo 10 de la ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal y en el artículo 9 del Código Tipo de la Unió Catalana d'Hospitals le recordamos que en el supuesto de que en el desarrollo de su relación laboral con nuestra empresa intervenga en cualquier fase del tratamiento de datos de carácter personal existentes en nuestros ficheros, está obligado al secreto profesional respecto de los mismos, y que esta obligación subsistirá incluso en el caso que finalizase su relación laboral con nuestra empresa.

ANEXO 6

I.- ***……encargado del tratamiento……*** se compromete a cumplir y hacer cumplir el deber de secreto profesional y de confidencialidad establecidos en el artículo 10 de la Ley Orgánica de Protección de Datos de Carácter Personal. Todo el personal de ***……encargado del tratamiento……***, que puedan tener acceso a documentación y datos está sujeto al más estricto secreto profesional en relación a los mismos. La obligación de secreto profesional por parte del ***……encargado del tratamiento……*** subsistirá incluso después de finalizar su relación con **……centro……**.

II.- ***……encargado del tratamiento……*** *se* compromete a tratar los datos de carácter personal o a los que tenga acceso en virtud de los servicios y trabajos que le sean encargados por ***……centro……*** únicamente conforme a las instrucciones facilitadas por este y a no aplicarlos o utilizarlos con otra finalidad; tampoco los comunicará en ningún caso a otras personas o entidades, de conformidad con lo establecido en el artículo 12.2 de la Ley Orgánica de Protección de Datos de Carácter Personal.

Asimismo ***……encargado del tratamiento……*** al finalizar la prestación contractual, o cuando así lo indique el responsable del tratamiento del ***……centro……***, se responsabilizará de que los datos de carácter personal sean conservados únicamente durante el tiempo que exija la normativa correspondiente y una vez transcurrido este, sean destruidos o retornados al igual que cualquier soporte donde consten, de conformidad con lo que establece el articulo 12.3 de la Ley Orgánica de Protección de Datos de Carácter Personal.

III.- ***……encargado del tratamiento……*** garantiza que, sin perjuicio del exacto cumplimiento de todo aquello que establece el presente documento, observará en todo momento, y en relación a los datos de carácter personal que le puedan ser facilitados por ***……centro……*** las disposiciones de la normativa sobre protección de datos de carácter personal.

ANEXO 7

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:_____
Dirección de la Oficina de Acceso: C/ _____ nº _____ C.P. _____
Localidad: _____ Provincia:_____

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 los artículos 15 de la Ley Orgánica 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94.

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 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, sin perjuicio de ejercer con carácter previo el derecho de queja ante el Comité Directivo del Código Tipo de la Unió Catalana d'Hospitals, en los términos establecidos en el artículo 20 del referido Código.

2. Que si la solicitud del derecho de acceso fuese estimada, se me remita por correo la comunicación favorable a la dirección arriba indicada a fin de que pueda ejercer el acceso en el término de 10 días, indicando a su vez las diferentes formas en que podré ejercer mi derecho.

3. Que estas formas en que podré ejercer el acceso comprendan 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

ANEXO 8

EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:_____
Dirección de la Oficina de Acceso: C/ _____ nº _____ C.P. _____
Localidad: _____ Provincia:_____

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 los artículos 16 de la Ley Orgánica 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 cinco 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 cinco días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley, sin perjuicio de ejercer con carácter previo el derecho de queja ante el Comité Directivo del Código Tipo de la Unió Catalana d'Hospitals, en los términos establecidos en el artículo 20 del referido Código.

En..... a..... de..... de 200.....

ANEXO 9

EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:_____
Dirección de la Oficina de Acceso: C/ _____ nº _____ C.P. _____
Localidad: _____ Provincia:_____

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 los artículos 16 de la Ley Orgánica 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA.

1. Que en el plazo de cinco días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.

2. 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 cinco días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley, sin perjuicio de ejercer con carácter previo el derecho de queja ante el Comité Directivo del Código Tipo de la Unió Catalana d'Hospitals, en los términos establecidos en el artículo 20 del referido Código

En..... a..... de..... de 200.....

ANEXO 10

EJERCICIO DEL DERECHO DE QUEJA

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:_____
Dirección de la Oficina de Acceso: C/ _____ nº _____ C.P. _____
Localidad: _____ Provincia:_____

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 queja, de conformidad con el artículo 19 del Código Tipo de la Unió Catalana d'Hospitals.

EXPONE.

1. Que ha tenido conocimiento de los siguientes hechos en relación al tratamiento de sus datos de carácter personal contenidos en el Fichero de Pacientes de su institución:

   _____
   _____
   _____

2. Que interesa que se constate la certeza de los hechos expuestos y en su caso se proceda a la rectificación de las actuaciones a que los mismos hacen referencia, con cumplida notificación al que suscribe de la resolución que se adopte.

En..... a..... de..... de 200.....

ANEXO 11

EJERCICIO DEL DERECHO DE QUEJA ANTE EL COMITÉ DIRECTIVO DEL CODIGO TIPO

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 queja ante el Comité Directivo del Código Tipo de la Unió Catalana d'Hospitals, de conformidad con el artículo 20 del mismo.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO DE LA ENTIDAD ADHERIDA AL CODIGO TIPO

Nombre:_____
Dirección de la Oficina de Acceso: C/ _____ nº _____ C.P. _____
Localidad: _____ Provincia:_____

EXPONE.

1. Que ha tenido conocimiento de los siguientes hechos en relación al tratamiento de sus datos de carácter personal contenidos en el Fichero de Pacientes de la referida institución:

   _____
   _____
   _____

2. Que ejerció el derecho de queja establecido en el artículo 19 del Código Tipo, tal como se acredita por medio de la copia con sello de entrada de la misma que se acompaña a este escrito.

3. *Que no está conforme con la resolución recaída de dicha queja, que se acompaña a este escrito / Que no ha recibido respuesta a la referida queja en el plazo de un mes desde su presentación.*

4. Interesa que por este Comité Directivo se proceda a incoar el preceptivo expediente y a través del mismo se constaten la certeza de los hechos objeto de queja y en su caso se proceda a requerir de la entidad adherida la rectificación de las actuaciones a que los mismos hacen referencia, con cumplida notificación al que suscribe de la resolución que se adopte.

En..... a..... de..... de 200.....

Documentos de Trabajo
del Grupo del Artículo 29

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

DG XV D/5057/97 final
WP 7

Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Documento de Trabajo: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?

Adoptado por el Grupo de Trabajo el 14 de enero de 1998

DOCUMENTO DE TRABAJO

EVALUACIÓN DE LA AUTORREGULACIÓN INDUSTRIAL: ¿EN QUÉ CASOS REALIZA UNA CONTRIBUCIÓN SIGNIFICATIVA AL NIVEL DE PROTECCIÓN DE DATOS EN UN PAÍS TERCERO?

Introducción

El apartado 2 del artículo 25 de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (95/46/CE) establece que el nivel de protección que ofrece un país tercero se evaluará atendiendo a *todas las circunstancias* que concurran en una transferencia o en una categoría de transferencias de datos. Se hace referencia específica no sólo a las normas de Derecho, sino también a las "normas profesionales y las medidas de seguridad en vigor en dichos países."

El texto de la Directiva exige por lo tanto que se tengan en cuenta las normas no jurídicas que puedan existir en el país tercero en cuestión, siempre que estas normas *estén vigentes.* En este contexto debe evaluarse la función de la autorregulación industrial.

¿Qué es la autorregulación?

El término "autorregulación" puede significar cosas distintas para diferentes personas. A efectos del presente documento, deberá entenderse por código de autorregulación (u otro instrumento) cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión.

Esta es una definición amplia que abarcaría desde un código de protección de datos voluntario desarrollado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos o banqueros, que suelen tener una fuerza cuasi jurídica.

¿Es el organismo responsable del código representante del sector?

Tal como sostendrá este documento, un importante criterio para juzgar el valor de un código es el grado hasta el cual pueden hacerse cumplir sus normas. En este contexto, la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos, tiene probablemente menos importancia que la fuerza de la asociación en cuanto a su capacidad de, por ejemplo, imponer sanciones a sus miembros por incumplimiento del código. No obstante, existen diversas razones secundarias que hacen que los códigos que abarcan a todo un sector industrial o una profesión sean instrumentos de protección más útiles que los desarrollados por pequeñas agrupaciones de empresas dentro de un sector industrial. En primer lugar figura el hecho de que, desde el punto de vista del consumidor, un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código para la protección de datos, es

algo confuso. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos sean objeto de tratamiento. En segundo lugar, especialmente en sectores tales como el marketing directo, donde es práctica corriente transferir los datos personales entre diferentes empresas del mismo sector, pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de ambigüedad en cuanto a la naturaleza de las normas aplicables, y también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

Evaluación de la autorregulación - el enfoque más adecuado

Dada la gran variedad de instrumentos que entran dentro de la noción de autorregulación, está claro que existe una necesidad de diferenciar entre las diversas formas de autorregulación en términos de su impacto real en el nivel de protección de datos aplicable cuando se transfieren datos personales a un país tercero.

El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos (tengan éstas categoría de autorregulación o de regulación) debe ser el enfoque general establecido en el documento de debate "Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación". La piedra angular de este enfoque es el examen no sólo del contenido del instrumento (deberá contener una serie de principios básicos), sino también de su eficacia en cuanto a lograr:

- un buen nivel de obediencia general
- apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento
- una reparación adecuada (incluida la compensación, cuando corresponda).

Evaluación del contenido de un instrumento de autorregulación

Esta es una tarea relativamente sencilla. Se trata de garantizar que estén presentes los "principios de contenido" necesarios establecidos en el documento "Primeras orientaciones" (véase el extracto adjunto). Esta es una evaluación objetiva. Se trata de ver cual es el contenido del código, y no cómo se elaboró éste. El hecho de que un sector industrial o profesión haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante por sí mismo, aunque evidentemente, si en su desarrollo se han tenido en cuenta las opiniones de los individuos cuyos datos sean objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje más fielmente los principios básicos necesarios para la protección de datos.

La transparencia del código es un elemento crucial; en particular, el código debería redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones.

Además, el código debería prohibir la transferencia de datos a empresas que no pertenezcan al sector y que no se rijan por el código, a menos que se prevean otras protecciones adecuadas.

Evaluación de la eficacia de un instrumento de autorregulación

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas por los que se garantiza la adhesión al código y por los que se resuelven los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales para juzgar la eficacia de la protección, para que pueda tenerse en cuenta un código de autorregulación en la evaluación de la adecuación de su protección.

Un buen nivel de obediencia general

Típicamente, un código profesional o industrial será desarrollado por un organismo representante del sector industrial o profesión en cuestión, y se aplicará a los miembros de dicho organismo representante específico. El nivel de cumplimiento del código dependerá del grado de conocimiento de la existencia del código y su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz, de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y, quizás lo más importante, de la naturaleza y la aplicación de las sanciones en caso de incumplimiento.
Por tanto, son importantes las siguientes preguntas:

- ¿Qué medidas adopta el organismo representante para asegurarse de que sus miembros conocen el código?
- ¿Exige el organismo representante a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
- ¿Presentan dichas pruebas las propias empresas o proceden de una fuente externa (tal como un auditor acreditado)?
- ¿Investiga el organismo representante las supuestas o presuntas violaciones del código?
- ¿Es el cumplimiento del código una condición para formar parte del organismo representante o es dicho cumplimiento meramente “voluntario”?
- En caso de que un miembro viole el código, ¿con qué tipos de sanciones disciplinarias cuenta el organismo representante (expulsión u otras)?
- ¿Es posible para un individuo o empresa continuar trabajando en la profesión o sector industrial concreto, incluso después de haber sido expulsado del organismo representante?
- ¿Puede hacerse cumplir el código de otras maneras, por ejemplo en los tribunales o en un tribunal especializado? Los códigos profesionales tienen fuerza jurídica en algunos países. En algunas circunstancias, también puede ser posible aplicar las leyes generales relativas a prácticas comerciales correctas o incluso de competencia para aplicar los códigos de conducta de los sectores industriales.

Al examinar los tipos de sanciones existentes, es importante distinguir entre una sanción “reparadora” que únicamente exige que un responsable del tratamiento, en caso de incumplimiento, modifique sus prácticas con el fin de adecuarlas a lo establecido en el código, y una sanción que vaya más lejos, castigando al responsable por su incumplimiento. Sólo la segunda categoría de sanción “punitiva” tiene repercusión en el comportamiento futuro de los responsables del tratamiento, proporcionando un incentivo para que se cumpla sistemáticamente el código.

La falta de sanciones auténticamente disuasorias y punitivas es por tanto un fallo esencial en un código. Sin dichas sanciones, es difícil entender cómo puede lograse un nivel satisfactorio de obediencia global, a no ser que se establezca un sistema riguroso de control externo (tal como una autoridad pública o privada competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

Apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento

Un requisito esencial para un sistema de protección de datos adecuado y eficaz es que no se abandone a los individuos que se enfrentan a un problema relativo a sus datos personales, sino que se les proporcione un apoyo institucional que permita hacer frente a sus dificultades. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:

- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Conlleva el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez sobre una supuesta violación de un código es un punto clave. Claramente, dicha persona u organismo deberá ser independiente respecto al responsable del tratamiento. No obstante, esto por sí mismo no basta para garantizar la imparcialidad. Idealmente, el árbitro debería asimismo no pertenecer a la profesión o sector en cuestión, por la razón de que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya violado el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

Reparación adecuada

Si el código de autorregulación resulta violado, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (p. ej. corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, permitir el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico o moral que se cause (llamado "distress" en el Derecho del Reino Unido y de EEUU).

Muchas de las cuestiones relativas a las sanciones que se han enumerado en la sección "Un buen nivel de obediencia general" son pertinentes aquí. Tal y como se ha

explicado anteriormente, las sanciones tienen una doble función: castigar al infractor (y fomentar así el cumplimiento de las normas por parte del infractor y de los demás), y remediar una violación de las normas. Nos ocuparemos ahora de la segunda función. Por lo tanto, podrían plantearse también las siguientes preguntas:

- ¿Es posible comprobar que un miembro que manifiestamente haya violado el código, ha modificado sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación con arreglo al código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una violación de contrato, o puede hacerse cumplir en virtud del Derecho público (p. ej. protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

Conclusiones

- La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el documento "Primeras orientaciones".
- Para que un instrumento de autorregulación pueda considerarse un elemento válido para una "protección adecuada" debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
- El instrumento debe ser transparente e incluir el contenido básico de los principios esenciales de la protección de datos.
- El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograr esto es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
- El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
- El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada.

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

XV D/5020/97- final
WP4

ANEXO

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación

Documento de debate adoptado por el Grupo de trabajo el 26 de junio de 1997

(i) Principios de contenido

Se sugiere la inclusión de los siguientes principios básicos:

1) **Principio de limitación de objetivos** - los datos deberán tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.

2) **Principio de proporcionalidad y de calidad de los datos -** los datos deberán ser exactos y, cuando sea necesario, estar actualizados. Los datos deberán ser adecuados, relevantes y no excesivos en relación al objetivo por el que se han transferido o por el que han sido nuevamente tratados.

3) **Principio de transparencia -** deberá informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el país tercero, y de cualquier otra cuestión siempre que resulte necesario para garantizar la equidad. Las únicas excepciones permitidas deberán corresponder a los artículos 11(2) y 13 de la Directiva.

4) **Principio de seguridad -** el responsable del tratamiento deberá adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no deberá tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición -** el interesado deberá tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado deberá también ser capaz de oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deberán estar en línea con el artículo 13 de la Directiva.

6) **Restricciones respecto a transferencias sucesivas a otros países terceros -** únicamente deberán permitirse transferencias sucesivas de datos personales del país tercero de destino a otro país tercero en el caso de que este último país tercero garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deberán estar en línea con el artículo 26 de la Directiva.

A continuación figuran ejemplos de principios adicionales que deberán aplicarse a tipos específicos de tratamientos:

1) **Datos sensibles -** cuando se trate de categorías de datos "sensibles" (las incluidas en el artículo 8), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) **Marketing directo -** en el caso de que el objetivo de la transferencia de datos sea el marketing directo, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) **Decisión individual automatizada -** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener el derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo del individuo.

11750/02/ES
WP 67

Documento de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara

Adoptado el 25 de noviembre de 2002

Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

Desempeña las labores de secretaría la Dirección A (Funcionamiento e Impacto del Mercado Interior, Coordinación y Protección de Datos) de la Dirección General de Mercado Interior de la Comisión Europea, B-1049 Bruxelles/Brussel, Bélgica. Despacho: C100-6/136.
Sitio web: www.europa.eu.int/comm/privacy

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[1],

Visto el artículo 29, así como la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su reglamento interno, y, en particular, sus artículos 12 y 14,

HA ADOPTADO EL PRESENTE DOCUMENTO DE TRABAJO:

1. INTRODUCCIÓN

Durante los últimos años, en Europa, los organismos públicos y privados han recurrido cada vez con más frecuencia a los sistemas de c aptación de imagen. Esta circunstancia ha suscitado un animado debate tanto en el ámbito comunitario como en los diferentes Estados miembros, a fin de determinar los requisitos y los límites relativos a la instalación de equipos destinados a la vigilancia por videocámara, así como las garantías necesarias para los interesados.

La experiencia vivida en los últimos años, a partir de la incorporación de la Directiva 95/46/CE en la legislación nacional, ha puesto de manifiesto la gran proliferación de sistemas de circuito cerrado, cámaras y otras herramientas más sofisticadas que se utilizan en los sectores más variados.

Asimismo, el desarrollo de la tecnología disponible, la digitalización y la miniaturización aumentan de manera considerable las oportunidade s que ofrecen los dispositivos de grabación de imagen y sonido, lo que también tiene que ver con su despliegue tanto en las intranets como en Internet.

Además de las operaciones de tratamiento de datos en el contexto laboral, que ya abordó el Grupo en un documento detallado, «Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral[2]», todos los ciudadanos pueden apreciar fácilmente la creciente proliferación de técnicas de vigilancia por videocámara.

Un análisis no exhaustivo de la s principales aplicaciones muestra que la vigilancia por videocámara puede servir para fines bastante diferentes[3], que, sin embargo, pueden agruparse en varias áreas principales:

---

1 DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.h tm

2 WP 48, adoptado el 13 de septiembre de 2001, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

3 Se han instalado diferente s sistemas de vigilancia por videocámara:
a) en el interior o en las proximidades de edificios públicos o abiertos al público, como museos, lugares de culto o monumentos, a fin de evitar delitos o actos vandálicos de importancia menor;

1) protección de las personas físicas;

2) protección de la propiedad;

3) interés público;

4) detección, prevención y control de delitos;

5) puesta a disposición de pruebas;

6) otros intereses legítimos.

Algunos requisitos también se refieren a la instalación de videocámaras y dispositivos similares.

En algunos casos, la utilización de un sistema de grabación de imagen puede ser, en realidad, obligatoria, de conformidad con disposiciones específicas de los Estados miembros (ha ocurrido, por ejemplo, en algunos casinos) o se realiza con un fin al que los familiares de los interesados conceden especial importancia (por ejemplo, en relación con la búsqueda de personas desaparecidas). Por otra parte, también se pueden citar ejemplos peculiares del uso de tales dispositivos (en particular, relativos a terceros países), como los casos en los que se han utilizado sistemas de reconocimiento fisonómico para impedir la bigamia o en los que una autoridad policial local ha decidido hacer públicas imágenes relativas a lo dura que es la vida en prisión para los presos, sin su consentimiento.

Por consiguiente, si bien la vigilancia por videocámara parece estar en cierto modo justificada en determinadas circunstancias, también se dan casos en los que se recurre a la protección mediante videocámaras de manera impulsiva, sin considerar adecuadamente los requisitos y medidas pertinentes. A veces, esto es debido a las ventajas económicas que conceden, en su mayoría, los organismos públicos, así como a las propuestas de mejores condiciones en materia de seguros derivadas de la utilización de equipos de vigilancia por videocámara.

---

b) en el interior de estadios y otras instalaciones deportivas, en particular cuando se celebran determinados acontecimientos;
c) en el sector del transporte y en relación con el tráfico rodado, con vistas a controlar el tráfico en carreteras y autopistas, a fin de detectar los excesos de velocidad o las violaciones del código de circulación en los centros urbanos, así como para controlar los subterráneos que dan acceso a las líneas del metro, vigilar las gasolineras y el interior de los taxis;
d) a fin de evitar o detectar conductas ilícitas en los alrededores de los colegios y en relación con los casos de menores importunados;
e) en el interior de los centros sanitarios, durante una operación o con vistas, por ejemplo, a dispensar cuidados a distancia o vigilar a los pacientes que se encuentran en unidades de cuidados intensivos o en áreas destinadas a pacientes gravemente enfermos o en cuarentena;
f) en aeropuertos, a bordo de barcos o cerca de las fronteras, para controlar el tráfico ilegal de extranjeros o para facilitar la búsqueda de menores u otras personas desaparecidas;
g) por parte de detectives privados;
h) en el interior y en las proximidades de supermercados y tiendas, en particular cuando venden artículos de lujo, con vistas a disponer de pruebas en caso de que se cometan delitos, así como para la comercialización de la mercancía o el establecimiento del perfil de los consumidores;
i) en el interior de las comunidades de vecinos y en zonas adyacentes, tanto por motivos de seguridad como para disponer de pruebas en caso de que se cometan delitos;
j) con fines periodísticos y publicitarios, que se prolongan en línea mediante cámaras *web* o cámaras virtuales que se utilizan con fines promocionales y publicitarios para el turismo, así como en relación con complejos turísticos y salas de baile, en los que se graba a los clientes y visitantes a intervalos regulares sin advertirles.

Así pues, se trata de un sector múltiple, en continua evolución, en el que ya hay varias técnicas disponibles.

El objetivo del presente documento de trabajo consiste en realizar un análisis inicial partiendo de la existencia de normativas parcialmente diferentes, así como de la presencia de disposiciones excesivamente detalladas en la legislación nacional de los diferentes Estados miembros, lo que requiere un enfoque más sistemático y armonizado.

El presente documento se refiere a la vigilancia destinada al control a distancia de acontecimientos, situaciones y sucesos, pero no tiene en cuenta directamente otros supuestos en los que determinados acontecimientos se divulgan de manera ocasional o tendenciosa en relación con la transparencia de la actividad de autoridades locales o instancias parlamentarias, por ejemplo.

A partir de ahí, cada operador podrá ampliar lo indicado aquí, tanto en relación con su sector correspondiente como en lo relativo a los avances tecnológicos futuros que el Grupo pretende investigar.

Asimismo, los principios que se incluyen en el presente documento se refieren a la captación de imágenes, si es posible combinadas con sonido o con datos biométricos, como huellas dactilares [4].

Dichos principios también podrán tenerse en cuenta, en los casos concretos en los que sea aplicable, en relación con el tratamiento de datos personales que no haya sido realizado con equipos de vídeo, sino mediante otros tipos de vigilancia, como control remoto (es el caso, por ejemplo, de los sistemas GPS por satélite).

El primer objetivo del presente documento es atraer la atención hacia la amplia gama de criterios que existen para evaluar la legalidad y la conveniencia de instalar sistemas individuales de vigilancia p or videocámara.

No obstante, también se han tenido en cuenta los siguientes aspectos:

a) Conviene que las instituciones pertinentes de los Estados miembros evalúen la vigilancia por videocámara desde un punto de vista general y con vistas a impulsar un enfoque globalmente selectivo, además de sistemático, para este asunto. La proliferación excesiva de sistemas de captación de imagen en zonas públicas y privadas no deberá traducirse en la imposición de restricciones injustificadas a los derechos y libert ades fundamentales de los ciudadanos; de lo contrario, los ciudadanos podrían verse obligados a someterse a procedimientos desproporcionados de recogida de datos que permitirían su identificación masiva en diversos lugares públicos y privados.

b) Las tendencias relativas a la evolución de las técnicas de vigilancia por videocámara podrían evaluarse de manera provechosa para evitar que el desarrollo de aplicaciones informáticas basadas tanto en el reconocimiento fisonómico como en el estudio y el pronósti co del comportamiento humano

[4] El Grupo tratará la cuestión más general de la aplicación de la Directiva 95/46/CE a los datos biométricos en un documento indepen diente.

reproducido conduzca de manera involuntaria a una vigilancia dinámico - preventiva, en contraposición con la vigilancia estática convencional, cuyo objetivo suele ser la documentación de acontecimientos específicos y de sus autores. Esta nueva forma de vigilancia está basada en la captación automatizada de los rasgos faciales de personas físicas y de su conducta «anormal» asociada a la disponibilidad de señales y avisos automatizados, lo que probablemente acarree riesgos de discriminación.

2. INSTRUMENTOS JURÍDICOS INTERNACIONALES

a) Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales

El artículo 8 del Convenio garantiza la protección del derecho a la intimidad.

b) Convenio nº 108/1981 del Consejo de Europa relativo a la protección de las personas físicas en lo que respecta al tratamiento automático de datos personales

El ámbito de aplicación de este Convenio no se limita, como la Directiva 95/46/CE, a las actividades del primer pilar (véase más adelante). Las actividades de vigilancia por videocámara que implican el tratamiento de datos personales entran en el ámbito de aplicación de este Convenio. El comité consultivo creado en virtud de este Convenio ha establecido que las voces y la imagen se considerarán datos personales cuando aporten información sobre una persona y la hagan identificable, incluso indirectamente.

En la actualidad, el Consejo de Europa está finalizando un conjunto de principios directores para la protección de las personas físicas en relación con la recogida y el tratamiento de datos a través de la vigilancia por videocámara. Dichos principios deberán profundizar en la especificación de las garantías relativas a los interesados, previstas en los instrumentos del Consejo de Europa.

c) Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la Unión Europea estipula, en su artículo 7, la protección de la vida privada y familiar, del domicilio y de las comunicaciones y en su artículo 8, la protección de los datos de carácter personal.

3. LA VIGILANCIA EN EL MARCO DE LA DIRECTIVA 95/46/CE

La Directiva 95/46/CE (de aquí en adelante «la Directiva») hace hincapié de manera expresa en las características específicas del tratamiento de la información personal incluida en los datos de sonido e imagen y se refiere a ellas expresamente en varios puntos.

Dicha Directiva garantiza la protección del derecho a la intimidad y la vida privada, así como la gama más amplia de protección de datos personales en lo que respecta a las libertades y los derechos fundamentales de las personas físicas (apartado 1 del artículo 1).

Una parte considerable de la información recogida mediante la vigilancia por videocámara se refiere a personas identificadas o identificables, que han sido filmadas mientras se encontraban en un lugar público o abierto al público. Es muy posible que la persona que se encuentra de paso se espere disfrutar de un menor grado de intimidad, pero lo que no se espera es verse totalmente desprovisto de sus derechos y libertades en lo que se refiere a su propia esfera e imagen.

También cabe tener en cuenta aquí el derecho a la libre circulación de las personas que se encuentran en el territorio de un Estado de manera legal, lo que se contempla en el artículo 2 del Protocolo Adicional nº 4 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Dicha libertad de circulación sólo puede estar sujeta a restricciones necesarias en una sociedad democrática y proporcionales a la consecución de fines específicos. Los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como el seguimiento de su conducta a causa de la utilización desproporcionada de la vigilancia por videocámara por parte de varias entidades en diversos lugares públicos o abiertos al público.

El carácter específico y sensible del tratamiento de datos constituidos por imagen y sonido relativos a personas físicas se pone de relieve en los primeros considerandos de la Directiva. Además de las consideraciones que se harán más adelante en cuanto al ámbito de aplicación, los considerandos mencionados y los artículos pertinentes de la Directiva aclaran lo siguiente:

a) en principio, la Directiva es aplicable a este asunto en vista también de la importancia del desarrollo de las técnicas utilizadas para captar, manejar y utilizar en cualquier otro modo la categoría específica de datos personales obtenidos de esta forma (véase el considerando 14);

b) los principios de protección de la Directiva también son aplicables a cualquier información (incluso la que esté constituida por imagen y sonido) relativa a una persona identificada o identificable, teniendo en cuenta el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquella (véanse la letra a) del artículo 2 y el considerando 26).

Además de las referencias específicas mencionadas, es obvio que la Directiva es plenamente aplicable en el marco de sus disposiciones individuales relativas, en concreto, a:

1) *Calidad de los datos*. Las imágenes serán tratadas de manera leal y lícita, y se destinarán a fines determinados, explícitos y legítimos. Se utilizarán de conformidad con el principio según

el cual los datos deberán ser adecuados, pertinentes y no excesivos, y no serán tratadas posteriormente de manera incompatible con dichos fines; se conservarán durante un período limitado, etc. (véase el artículo 6).

2) *Principios relativos a la legitimación del tratamiento de datos.* En base a estos principios, es necesario que el tratamiento de datos personales mediante vigilancia por videocámara esté fundamentado en al menos uno de los requisitos mencionados en el artículo 7 (consentimiento inequívoco, necesidad de obligaciones contractuales, de cumplimiento de una obligación jurídica, de protección del interés vital del interesado, de cumplimiento de una misión de interés público o inherente al ejercicio del poder público, equilibrio de intereses, etc.).

3) Tratamiento de *categorías especiales de datos*, sujeto a las garantías aplicables al uso de datos se nsibles o datos relativos a infracciones en el marco de la vigilancia por videocámara (con arreglo al artículo 8).

4) *Información* que se facilitará al interesado (véanse los artículos 10 y 11).

5) *Derechos del interesado*, en concreto el derecho de acceso y el derecho de oposición al tratamiento por razones legítimas (véase el artículo 12 y la letra a) del artículo 14).

6) Garantías aplicables en relación con *las decisiones individuales automatizadas* (véase el artículo 15).

7) *Seguridad* de las operaciones de tratamiento (véase el artículo 17).

8) *Notificación de las operaciones de tratamiento* (véanse los artículos 18 y 19).

9) *Controles previos* de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (véase el artículo 20).

10) *Transferencia de datos a terceros países* (artículo 25 y siguientes).

El carácter específico y sensible del tratamiento de datos constituidos por imagen y sonido se reconoce finalmente en el último artículo de la Directiva, a través del cual la Comisión se compromete a estudiar, en particular, la aplicación de la directiva a dicho asunto y a presentar las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información (véase el artículo 33).

4. DISPOSICIONES NACIONALES APLICABLES A LA VIGILANCIA POR VIDEOCÁMARA

En varios Estados miembros ya se han realizado estudios de casos relativos a la vigilancia por videocámara, basados tanto en dispo siciones constitucionales [5] como en

[5] Véase la sentencia 255/2002 del Tribunal Constitucional de Portugal, con arreglo a la cual el Tribunal determinó que «la utilización de dispositivos de vigilancia electrónica y el control de

legislación específica o en resoluciones y otras decisiones emitidas por las autoridades nacionales competentes [6].

En algunos países también existen disposiciones específicas aplicables independientemente del hecho de que la vigilancia por videocámara pueda implicar el tratamiento de datos personales. Con arreglo a dicha normativa, la instalación y el despliegue de circuitos cerrados de televisión y equipos de vigilancia similares deberán ser autorizados previamente por una autoridad administrativa (que podrá estar representada, parcialmente o a todos los efectos, por la autoridad nacional de protección de datos). Dicha normativa podrá diferir en función de la naturaleza pública o privada de la entidad responsable de maneja r el equipo en cuestión.

En otros países, la vigilancia por videocámara no es objeto de legislación específica en la actualidad; sin embargo, las autoridades de protección de datos han estado trabajando para garantizar la aplicación adecuada de las dispo siciones generales de protección de datos, en particular a través de dictámenes, directrices o códigos de conducta (que ya han sido adoptados en el Reino Unido y están siendo elaborados en Italia, por ejemplo).

Bélgica	Dictámenes de la autoridad de protección de datos, en concreto, el Dictamen 34/99, de 13 de diciembre de 1999, relativo al tratamiento de imágenes, en particular a través de la utilización de sistemas de vigilancia por videocámara; el Dictamen 3/2000, de 10 de enero de 2000, relativo a la utilización de sistemas de vigilancia por videocámara en la entrada de los edificios de apartamentos.
Dinamarca	Texto refundido de la Ley nº 76, de 1 de febrero de 2000, relativa a la prohibición de la vigilancia por videocámara. Resolución de la autoridad de protección de datos, de 3 de junio de 2002, relativa a la vigilancia por videocámara por parte de un gran grupo de supermercados y transmisión en directo desde un *pub* a través de Internet.
Francia	Ley 78-17, de 6 de enero de 1978, relativa a la informática, los archivos y las libertades (Comisión nacional francesa de informática y libertades, CNIL). Recomendación 94-056 de la autoridad de protección de datos, de 21 de junio de 1994.

ciudadanos por parte de organismos privados de seguridad constituye un límite o una restricción al derecho a preservar la vida privada, consagrado en el artículo 26 de la Constitución».

6 Al menos en un país (Bélgica, caso Gaia), el incumplimiento de la legislación relativa a la protección de datos en el marco de la captación de imágenes ha llevado al rechazo de pruebas admisibles ante el Tribunal.

	Directrices de la autoridad de protección de datos relativas a la vigilancia por videocámara en el lugar de trabajo: http://www.cnil.fr/thematic/index.htm ; sobre otros asuntos (como la cámara *web*)[7]. Ley específica relativa a la vigilancia por videocámara para la seguridad pública en zonas públicas: Ley 95-73, de 21 de enero de 1995, sobre seguridad (modificada por la Orden 2000-916, de 19 de septiembre de 2000). Decreto 96-926, de 17 de octubre de 1996 y Circular, de 22 de octubre de 1996, sobre la aplicación de la Ley 95-73.
Grecia	Resolución de la autoridad de protección de datos de 28 de enero de 2000 (sobre el metro de Atenas).
Alemania	Letra b de la sección 6 de la Ley federal de 2001.
Irlanda	Estudio de casos nº 14/1996 (utilización de circuitos cerrados de televisión).
Italia	Sección 20 del Decreto legislativo nº 467, de 28 de diciembre de 2001 (relativa a la adopción de códigos de conducta). Resoluciones de la autoridad italiana de protección de datos: nº 2, de 10 de abril de 2002 (relativa al fomento de la adopción de códigos de conducta), de 28 de septiembre de 2001 (relativa a las técnicas biométricas y de reconocimiento fisonómico aplicadas por los bancos) y de 29 de noviembre de 2000 (el llamado «decálogo de la vigilancia por videocámara»). Decreto presidencial nº 250, de 22 de junio de 1999 (por el que se regula el acceso de vehículos a los centros urbanos y a las zonas de acceso restringido). Decreto nº 433, de 14 de noviembre de 1992, y Ley nº 4/1993 (relativa a museos, bibliotecas públicas y archivos). Decreto legislativo nº 45, de 4 de febrero de 2000 (barcos de pasajeros en rutas nacionales). Sección 4 de la Ley nº 300, de 20 de mayo de 1970 (el llamado «Estatuto de los trabajadores»).
Luxemburgo	Artículos 10 y 11 de la Ley de 2 de agosto de 2002, relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales.
Países Bajos	Informe de la autoridad de protección de datos publicado en 1997, que contiene las directrices para

[7] Véanse los informes anuales de la Comisión nacional francesa de informática y libertades (CNIL).

	la vigilancia por videocámara, en parti cular para la protección de las personas físicas y la propiedad en lugares públicos. Recientemente, la Cámara baja aprobó un proyecto de Ley por el que se ampliará el alcance del delito de grabar imágenes de lugares abiertos al público sin informar al mi smo. En breve se transmitirá al Parlamento un proyecto de Ley por el que se atribuirán competencias explícitas a los ayuntamientos para utilizar sistemas de vigilancia por videocámara en determinadas condiciones.
Portugal	Decreto ley nº 231/98, de 22 de julio de 1998 (relativo a la actividad privada en materia de seguridad y a los sistemas de autoprotección). Ley nº 38/98, de 4 de agosto de 1998 (relativa a las medidas que deberán adoptarse en caso de violencia relacionada con acontecimientos deportivos) . Decreto ley nº 263/01, de 28 de septiembre de 2001 (relativo a las zonas de baile). Decreto ley nº 94/2002, de 12 de abril de 2002 (acontecimientos deportivos).
España	Ley Orgánica nº 4/1997 (por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos). Real Decreto nº 596/1999, por el que se aplica la Ley Orgánica nº 4/1997.
Suecia	La vigilancia por videocámara se regula de manera específica en la Ley 1998/150 sobre vigilancia general por videocámar as y la Ley 1995/1506 sobre vigilancia secreta por videocámara (en indagaciones criminales) [8].

[8] En Suecia, aunque la vigilancia general por videoc ámara requiere, en principio, autorización de la junta administrativa municipal, existen varias excepciones, por ejemplo, en lo relativo a la vigilancia de oficinas de correos, bancos y tiendas. La vigilancia secreta por videocámara debe contar con la autorización de un tribunal. A fin de preservar intereses públicos, el Ministro de Justicia puede apelar una sentencia de la junta administrativa municipal dictada de conformidad con la Ley sobre vigilancia general por videocámara. Se considera que la grabación de imágenes utilizando cámaras digitales constituye tratamiento de datos personales en el sentido contemplado en la Ley sueca sobre datos personales y, en consecuencia, entra en el marco de la supervisión por parte de la autoridad de protección de datos. En la actualidad, un comité de investigación está analizando la utilización de vigilancia por videocámara desde una perspectiva de prevención criminal. Entre otras cosas, dicho comité evaluará la Ley sobre vigilancia general por videocámara a fin de verif icar si es necesario introducir modificaciones. Asimismo, el comité de investigación analizará el ámbito de aplicación de la Ley sueca de datos personales en lo que respecta a la vigilancia por videocámara y la posible necesidad de establecer normas especí ficas relativas al tratamiento de datos personales en relación con la vigilancia por videocámara.

Reino Unido	Código profesional 2000 sobre circuitos cerrados de televisión (Delegado de Información).

También se han adoptado instrumentos reguladores import antes en Islandia (sección 4 de la Ley nº 77/2000), Noruega (título VII de la Ley nº 31, de 14 de abril de 2000), Suiza (recomendación del Delegado federal) y Hungría (recomendación de la autoridad de protección de datos, de 20 de diciembre de 2000).

5. ÁREAS EN LAS QUE LA DIRECTIVA 95/46/CE NO ES APLICABLE EN TODO O EN PARTE

La Directiva no es aplicable al tratamiento de datos constituidos por imagen y sonido cuando éstos se utilizan con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado en ámbitos del Derecho penal, así como para el ejercicio de otras actividades que no están comprendidas en el ámbito de aplicación del Derecho comunitario [9]. No obstante, al incorporar la Directiva 95/46/CE en la normativa nacional, muchos Estados miembros cubrieron estos ámbitos de manera general, aunque estipularon excepciones específicas.

A) En cualquier caso, en algunos países, las operaciones de tratamiento realizadas con los fines mencionados anteriormente también están sujetas a garantías, en cumplimiento del Convenio nº 108/1981 y de las recomendaciones pertinentes del Consejo de Europa, así como de determinadas disposiciones nacionales (véase el apartado 2 del artículo 3 y el considerando 16 de la Directiva 95/46/CE). A la luz de estas características peculiares y de la existencia de disposiciones específicas también relacionadas con las actividades de investigación llevadas a cabo por autoridades policiales y judiciales, así como con fines de seguridad del Estado[10] (que pueden incluir vigilancia por videocámara «oculta», es decir, realizada sin informar sobre el lugar), esta categoría de operaciones de tratamiento no se abordará de manera detallada en el presente documento.

No obstante, al Grupo le gustaría destacar que, al igual que algunas otras operaciones de tratamiento de datos personales que tampoco están comprendidas en el ámbito de aplicación de la Directiva, la vigilancia por videocámara realizada por motivos de necesidad real de seguridad pública o para la detección, prevención y control de delitos deberá cumplir los requisitos establecidos en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales y, en ambos casos, estar cubierta por disposiciones específicas conocidas por el público, estar relacionada con la prevención de riesgos *concretos* y delitos *específicos* y ser proporcional a éstos (por ejemplo, en locales expuestos a tales riesgos o en relación con acontecimientos públicos los cuales es

[9] Véase el considerando 16.

[10] Cabe hacer referencia aquí a los principios establecidos por el Tribunal Europeo de Derechos Humanos en el asunto Rotaru contra Rumania, examinado el 4 de mayo de 2000. Véase más arriba.

razonablemente posible que den lugar a tales delitos [11]). Deberán tenerse en cuenta los efectos que producen los sistemas de vigilancia por videocámara (por ejemplo, el hecho de que las actividades ilegales puedan trasladarse a otras áreas o sectores) y deberá especificarse siempre claramente quién es el responsable del tratamiento, a fin de que los interesados puedan ejercer sus derechos.

Éste último requisito también tiene que ver con el hecho de que cada vez es más frecuente que la vigilancia por videocámara la realicen conjuntamente la policía y otras autoridades públicas (por ejemplo, autoridades locales) o entidades privadas (bancos, asociaciones deportivas, empresas de transporte, etc.), lo que conlleva un riesgo de confusión en cuanto al papel y la responsabilidad individuales en relación con las tareas que se van a realizar [12].

B) En segundo lugar, la Directiva no es aplicable a las operaciones de tratamiento realizadas por una persona física en el marco de una actividad meramente personal o familiar (véase el apartado 2 del artículo 3 y el considerando 12).

Si bien este supuesto puede ser pertinente cuando, por ejemplo, la vigilancia por videocámara la realiza una persona para controlar a distancia lo que ocurre dentro de su propia casa (por ejemplo, para evitar robos o en relación con la gestión de la llamada «e-family»), no ocurre lo mismo cuando el equipo de vigilancia por videocámara se ha instalado en el exterior de la casa o en las proximidades de un local privado, con vistas a proteger la propiedad o a garantizar la seguridad.

En este caso puede ser, en primer lugar, que el sistema no lo hayan puesto en marcha propietarios individuales para vigilar las puertas que dan acceso a su propiedad, sino más bien varios propietarios, con arreglo a un acuerdo, o un consorcio o comunidad de vecinos, con el objeto de controlar varias entradas y áreas de un bloque, lo que hace que la Directiva sea aplicable a las actividades pertinentes.

Siempre que el sistema se utilice en beneficio de un hogar individual y con el objeto de controlar una única puerta, un único descansillo, aparcamiento, etc., el hecho de que la Directiva no sea aplicable debido a su utilización exclusivamente personal, así como a la indisponibilidad de los datos para terceras partes, no exime al responsable del tratamiento de respetar los derechos e intereses legítimos de sus vecinos y demás personas de paso. En los Estados miembros de la UE, en realidad, estos derechos e intereses

---

11 Por ejemplo, una circular emitida en Francia el 22 de octubre de 1996 relativa a los lugares aislados y las tiendas que cierran tarde por la noche.

12 Un ejemplo significativo de este riesgo lo constituyen las actividades que llevan a cabo varios municipios de Italia a fin de controlar, mediante vigilancia por videocámara, zonas públicas frecuentadas por la noche por prostitutas. En el pasado, algunos municipios reclamaron su competencia en la prevención de este fenómeno (lo cual es discutible), mientras que otros únicamente emitieron mandatos en los que se prohibía a los clientes de las prostitutas aparcar o conducir sus vehículos en esas zonas y se les amenazaba con enviar una fotografía a sus hogares si no obedecían. La autoridad competente italiana ha adoptado una decisión a fin de aclarar cuáles son las medidas adecuadas para la acusación de violación de las disposiciones pertinentes.

están protegidos, independientemente de los principios de la protección de datos, por las disposiciones generales (código civil) que protegen los derechos, la imagen, la vida familiar y el ámbito privado de las personas (pensemos, por ejemplo, en el ángulo visual de una cámara instalada en el exterior de un apartamento, lo que permite grabar, sistemáticamente, a los clientes de una clínica o un bufete de abogados situados en el mismo piso y, de este modo, inmiscuirse de manera ilegal en el secreto profesional).

Deberá prestarse especial atención a la orientación del equipo de vídeo, a la obligación de enviar avisos e información y al borrado oportuno de las imágenes (en el plazo de unas horas) si no se ha producido allanamiento de morada ni otros delitos.

C) Por último, en el artículo 9 de la Directiva se estipula que los Estados miembros establecerán exenciones y excepciones respecto de algunas de las disposiciones cuando el tratamiento se realice con fines exclusivamente periodísticos o de expresión artística o literaria, en particular en el sector audiovisual (véase el considerando 17). Sólo se establecerán excepciones en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión [13]. En este sentido, se prestará especial atención a la hora de instalar cámaras *web* o cámaras virtuales, a fin de evitar defectos y carencias en la protección de las personas físicas en el marco de la vigilancia por videocámara con fines que resulte que consisten en actividades publicitarias o de promoción turística [14].

6. VIGILANCIA POR VIDEOCÁMARA Y TRATAMIENTO DE DATOS PERSONALES

A la luz de las diversas situaciones mencionadas, el Grupo considera necesario llamar la atención sobre el hecho de que la Directiva 95/46/CE es aplicable al tratamiento total o parcialmente automatizado de datos personales, incluidos los constituidos por imagen y sonido captados mediante circuito cerrado de televisión y otros sistemas de vigilancia por videocámara, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Los datos relativos a personas físicas identificadas o identificables, constituidos por imagen y sonido, son datos personales:

a) incluso si las imágenes se utilizan en el marco de un sistema de circuito cerrado y aunque no estén asociadas a los datos personales del interesado;

b) incluso si no se refieren a personas cuyos rostros hayan sido filmados, aunque contengan otra información, como, por ejemplo,

---

13 Véase la Recomendación 1/97 del Grupo sobre la Ley de protección de datos y los medios.

14 Una cámara *web* instalada subrepticiamente cerca de las escaleras que conducen a la salida de una estación de metro de Milán mostraban directamente en la red imágenes de las partes íntimas de mujeres que pasaban por ahí, con fines aparentemente relacionados con actividades periodísticas. El hecho de que las personas implicadas no pudieran ser identificadas evitó que la autoridad nacional de protección de datos tomara medidas en el asunto.

números de matrícula o números de identificación personal (PIN) captados durante la vigilancia de cajeros automáticos;

c) independientemente del método utilizado para el tratamiento (por ejemplo, sistemas de vídeo fijos o móviles, como receptores de imagen portátiles, o imágenes en color o en blanco y negro), la técnica (dispositivos de cable o fibra óptica), el tipo de equipo (fijo, móvil o portátil), las características de la captación de imágenes (es decir, continua por oposición a discontinua, lo que ocurre, por ejemplo, cuando la captación de la imagen sólo se realiza en caso de que no se respete el límite de velocidad y no tiene nada que ver con la grabación de imágenes realizada de manera totalmente fortuita y poco sistemática) y las herramientas de comunicación utilizadas (por ejemplo, la conexión con un «centro» o el envío de imágenes a terminales remotos).

A efectos de la Directiva, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dis positivos específicos.

Por lo tanto, una de las primeras precauciones que deberá tomar el responsable del tratamiento es verificar si la vigilancia por videocámara implica el tratamiento de datos personales relacionados con personas identificables. En es e caso, la Directiva es aplicable, independientemente de las disposiciones nacionales en las que se requiera, además, autorización por motivos de seguridad pública.

Este puede ser el caso, por ejemplo, cuando se trate de equipos colocados a la entrada o en el interior de un banco, cuando dichos equipos permitan identificar a los clientes; por el contrario, en determinadas circunstancias, la Directiva dejará de ser aplicable cuando se trate de imágenes captadas durante un reconocimiento aéreo, que no puedan ser ampliadas de manera provechosa o no incluyan información relativa a personas físicas (como puede ocurrir cuando las imágenes se recogen para identificar manantiales o zonas de vertido de residuos), o en el caso de imágenes de barrido del tráfico en l as autopistas.

7. OBLIGACIONES Y PRECAUCIONES ADECUADAS RELATIVAS AL RESPONSABLE DEL TRATAMIENTO DE DATOS

A) Legalidad del tratamiento

Habida cuenta de que el tratamiento deberá ser lícito (véase la letra a) del artículo 6 de la Directiva), el responsable d el tratamiento verificará previamente si la vigilancia cumple las disposiciones generales y específicas del sector (como leyes, reglamentos o códigos de conducta con pertinencia legal). Dichas disposiciones también han podido establecerse por motivos de seguridad pública o por motivos diferentes a los relativos a la protección de datos personales (por ejemplo, la necesidad de obtener autorizaciones *ad hoc* por parte de organismos administrativos específicos y de cumplir sus instrucciones).

Se tomarán todas las medidas adecuadas para garantizar que la vigilancia por videocámara cumple los principios de la protección de datos, y se evitarán las referencias inadecuadas a la intimidad [15].

En este sentido, también se tendrán en cuenta las buenas prácticas que fi guren en las recomendaciones elaboradas por autoridades de control o en otros instrumentos de autorregulación.

Conviene, también, verificar las demás disposiciones nacionales (incluidos los principios constitucionales y los códigos civiles y penales), en particular las que se refieren al «derecho a la imagen» [16] o a la protección del domicilio propio; deberá tenerse en cuenta la jurisprudencia pertinente, en la que es posible que se establezca que algunos lugares fuera del hogar (como habitaciones de hotel, oficinas, aseos, cabinas telefónicas interiores, etc.) se considerarán lugares privados.

Cuando el equipo haya sido instalado por entidades privadas o por organismos públicos, en particular por autoridades locales, supuestamente por motivos de seguridad o para detectar, prevenir y controlar delitos, se prestará especial atención, a la hora de determinar dichos motivos o informar sobre ellos, a las tareas que debe realizar el responsable del tratamiento con arreglo a la normativa (teniendo en cuenta que, según la normativa, determinadas funciones públicas sólo pueden ser ejercidas por organismos no administrativos específicos, en concreto, por la autoridad competente).

Esta cuestión se ha planteado de manera específica con respecto a unas cuantas autoridades locales que no tienen competencia directa en los asuntos del orden público y la seguridad pública, y que, no obstante, realizan actividades auxiliares destinadas a la vigilancia. De la misma forma, la vigilancia, para cuya justificación se suele aducir su utilización en el control de la delincuencia, en realidad tiene como objetivo aportar pruebas en caso de que se cometan delitos.

B) Especificidad, especificación y legalidad de los fines

El responsable del tratamiento se asegurará de que los fines sean claros e inequívocos, también con el objeto de ofrecer un criterio preciso a la hora de evaluar la compatibilidad de los fines perseguidos por el tratamiento (véase la letra b) del artículo 6 de la Directiva).

Esta claridad también es necesaria con vistas a enumerar los fines, tanto en la información que se facilitará a los interesados como en la notificación pertinente, así como en lo relativo al control previo que posiblemente se lleve a cabo en relación con el tratamiento, de conformidad con el artículo 20 de la Directiva.

---

15 Recientemente, un banco y una comisaría local fueron incapaces de satisfacer la solicitud de un cliente, que pedía que, de las imágenes grabadas por una cámara que también filmaba un cajero automático, se extrajeran las correspondientes a un ladrón que, tras robar la tarjeta de crédito del cliente, la había utilizado para sacar dinero ilegalmente en dicho cajero (por motivos supuestamente relacionados con la «intimidad»).

16 En Francia y en Bélgica, este derecho requiere «consentimiento previo».

Quedará claramente excluido que las imágenes captadas puedan ser utilizadas con otros fines, en concreto en lo que se refiere a las posibilidades técnicas de reproducción (por ejemplo, prohibiendo expresamente su copia).

Se hará referencia a los fines pertinentes en un documento en el que también se resumirán otras características importantes de la política de privacidad (respecto a cuestiones tan importantes como el momento en que se borran las imágenes, las posibles peticiones de acceso por parte de los interesados y la consulta lícita de los datos).

C) Principios relativos a la legitimación del tratamiento de datos

El responsable del tratamiento verificará que la vigilancia por videocámara no sólo cumple las disposiciones específicas a las que se hace referencia en el apartado A), sino también, como mínimo, uno de los principios relativos a la legitimación del tratamiento de datos que figuran en el artículo 7 de la Directiva (con relación específica a la protección de datos personales).

Aparte de los casos, menos frecuentes, en los que debe cumplirse una obligación legal (se ha hecho referencia a las actividades en un casino) o en los que el tratamiento es necesario para proteger intereses vitales (por ejemplo, para el control a distancia de pacientes en unidades de reanimación), a menudo es necesario que el responsable del tratamiento cumpla una misión de interés público o inherente al ejercicio del poder público, posiblemente a través del cumplimiento de normativa específica (por ejemplo, para detectar delitos de tráfico o comportamientos violentos en medios de transporte públicos en zonas de alta criminalidad), con arreglo a la letra e) del artículo 7 de la Directiva; por otra parte, el responsable del tratamiento puede perseguir un interés legítimo sobre el que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado (véase la letra f) del artículo 7).

En ambos casos y, en particular, en éste último, la naturaleza sensible de las operaciones de tratamiento requiere un análisis minucioso del ámbito de las misiones, los poderes y los intereses legítimos relativos al responsable del tratamiento. A la hora de realizar dichos análisis, deberán evitarse totalmente la superficialidad y la extensión sin fundamento del ámbito de dichas misiones y poderes.

En lo que se refiere, en concreto, al equilibrio entre los diferentes intereses, deberá prestarse especial atención (escuchando previamente a las partes interesadas) a la posibilidad de que un interés que merezca protección pueda entrar en conflicto con la instalación del sistema o con determinados acuerdos de retención de datos u otras operaciones de tratamiento[17].

Por último, en lo relativo a la obtención del consentimiento del interesado, éste último deberá ser inequívoco y estar basado en información clara. El consentimiento

[17] En la letra b de la sección 6 de la nueva Ley federal alemana de protección de datos, que entró en vigor el 23 de mayo de 2001, la observación de zonas abiertas al público mediante dispositivos ópticos y electrónicos está permitida si, entre otras cosas, no hay motivos para pensar que prevalecen intereses del titular de los datos que deben ser protegidos.

se otorgará por separado y estará específicamente vinculado a las actividades de vigilancia relativas a un lugar en el que se desarrolle la vida privada de una persona [18].

La legalidad del tratamiento se evaluará teniendo en cuenta las disposiciones de la Directiva por las que se establecen garantías específicas en cuanto al tratamiento de datos relativos a infracciones (véase el apartado 5 del artículo 8 de la Directiva) [19].

Cuando las operaciones de tratamiento mediante vigilancia por videocámara las llevan a cabo organismos públicos, deberán basarse siempre en disposiciones legales específicas.

D) Proporcionalidad del recurso a la vigilancia por videocámara

El principio según el cual los datos deberán ser adecuados y proporcionales al fin perseguido significa, en primer lugar, que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir:

1. Con fines que realmente justifiquen el recurso a tales sistemas.

   Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos).

   Dicho de otro modo, es necesario aplicar, caso por caso, el *principio de idoneidad* con respecto a los fines perseguidos, lo que implica una especie de *obligación de minimización de los datos* por parte del responsable del tratamiento.

   Si bien un sistema proporcionado de vigilancia por videocámara y alerta puede considerarse lícito cuando se cometen agresiones repetidas a bordo de autobuses en zonas periféricas o cerca de las paradas de autobús, no ocurre lo mismo cuando se trata de un sistema destinado a evitar que se insulte a los conductores de autobús o que se ensucien los vehículos (tal y como le ha sido descrito a una autoridad de protección de datos) o, incluso, a identificar a ciudadanos responsables de infracciones de menor importancia, como dejar las bolsas de basura fuera del cubo o en zonas en las que está prohibido tirar basura.

   La proporcionalidad deberá evaluarse basándose en criterios más estrictos en lo que se refiere a lugares cerrados al público.

---

[18] Se prestará especial atención a la posibilidad real de manifestar un consentimiento válido en el sentido contemplado en la letra h) del artículo 2 de la Directiva 95/46/CE («toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan») en caso de instalación de vigilancia por videocámara en una copropiedad (comunidad de vecinos, etc.).

[19] Cabe hacer referencia aquí al artículo 8 de la Ley portuguesa nº 67/98 en lo relativo a los datos concernientes a personas sospechosas de haber participado en actividades ilegales o criminales.

El intercambio de información y experiencias entre las autoridades competentes de los diferentes Estados miembros puede ser útil en este sentido[20].

2. Además, podrán utilizarse estos sistemas si otras medidas de protección y seguridad que no implican captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de limpieza, sistemas combinados de alarma, mejores sistemas de alumbrado nocturno en las calles, etc.) resultan claramente insuficientes o inaplicables en relación con los fines legítimos mencionados más arriba.

Las consideraciones anteriores se refieren, en concreto, al uso cada vez más frecuente de vigilancia por videocámara con fines de autodefensa y protección de la propiedad (sobre todo, cerca de edificios públicos y oficinas, incluidas las áreas circundantes). Para este tipo de utilización se requiere la evaluación, desde un punto de vista más general, de los efectos indirectos derivados del recurso masivo a la vigilancia por videocámara (es decir, si la instalación de varios dispositivos es realmente un factor disuasorio o si los infractores o vándalos pueden, simplemente, desplazarse a otras zonas y actividades).

E) Proporcionalidad en la realización de actividades de vigilancia por videocámara

El principio según el cual los datos deben ser adecuados, pertinentes y no excesivos implica la evaluación minuciosa de la *proporcionalidad de las medidas* relativas al tratamiento de datos, una vez que la legalidad del mismo haya quedado validada.

Las *medidas para la grabación* se establecerán teniendo en cuenta, en primer lugar, los siguientes aspectos:

a) El ángulo visual con arreglo a los fines perseguidos[21] (por ejemplo, si la vigilancia se realiza en un lugar público, el ángulo deberá establecerse de manera que no permita visualizar detalles o rasgos físicos que resulten irrelevantes para los fines perseguidos, o zonas situadas en el interior de lugares privados cercanos, en particular, si se utiliza el zoom).

b) El tipo de equipo que se utilizará para filmar, es decir, fijo o móvil.

---

20 Esto permitiría, además, armonizar mejor los enfoques reguladores y las decisiones administrativas, que, en algunos casos, no se han puesto de acuerdo (como ha ocurrido, por ejemplo, con las salas de bingo).

21 Se pueden encontrar ejemplos de precauciones específicas que deben tomarse en relación con el ángulo visual en dos disposiciones de la autoridad italiana de protección de datos. Un organismo de asistencia sanitaria tenía previsto crear un sistema que permitiese que los familiares de pacientes en coma, en cuarentena o con enfermedades graves, tratados en unidades de cuidados intensivos, pudieran observarlos continuamente desde la distancia, por lo que se comunicó a dicho organismo que debería tomar las medidas necesarias para evitar la visualización simultánea de otros pacientes. En otro caso, la autoridad señaló a los órganos administrativos de la policía que un sistema para la detección del exceso de velocidad sólo podía filmar las matrículas pertinentes y no el interior de los vehículos.

c) Medidas reales de instalación, es decir, situación de las cámaras, utilización de plano fijo o cámaras móviles, etc.

d) Posibilidad de aumentar las imágenes o realizar primeros planos, durante la grabación o después, es decir, una vez que se han almacenado las imágenes.

e) Congelación de imágenes.

f) Conexión con un «centro» para enviar señales de alarma sonoras o visuales.

g) Medidas que se toman como resultado de la vigilancia por videocámara, es decir, cierre de entradas, convocatoria del personal de vigilancia, etc.

En segundo lugar, deberá tenerse en cuenta la *decisión que se va a tomar en cuanto a la retención de las imágenes y el plazo* (éste último deberá ser bastante breve y estar en consonancia con las características específicas de cada caso).

Si bien en algunos casos un sistema que sólo permita la visualización de imágenes en circuito cerrado, sin necesidad de grabar, puede ser suficiente (por ejemplo, en el caso de las cajas de un supermercado), en otros (por ejemplo, para proteger lugares privados), puede que esté justificado grabar imágenes durante unas cuantas horas y borrarlas automáticamente, sin exceder nunca el final del día o, como mucho, el final de la semana. Obviamente, esta regla tiene excepciones, como cuando se emite una señal de alarma o se realiza una petición que merece especial atención; en esos casos, hay motivos suficientes para esperar, durante un período breve, una posible decisión por parte de las autoridades policiales o judiciales.

Por poner otro ejemplo, un sistema cuyo objetivo es detectar el acceso no autorizado de vehículos a centros urbanos y zonas de tráfico restringido, sólo deberá grabar imágenes en caso de que se cometa una infracción.

La cuestión de la proporcionalidad también deberá tenerse en cuenta debidamente siempre que se considere que son necesarios períodos de retención más breves, que no deberán superar una semana[22] (por ejemplo, imágenes de vigilancia por videocámara que puedan utilizarse para identificar a las personas que frecuentan un banco antes de que se cometa un robo).

En tercer lugar, deberá prestarse atención a los *casos en los que se facilita la identificación de una persona* mediante la asociación de imágenes del rostro de dicha persona con otra información relativa a conductas o actividades reproducidas (por ejemplo, en caso de asociación de imágenes y actividades realizadas por los clientes de un banco en un momento fácilmente identificable).

En este sentido, deberá tenerse en cuenta la clara diferencia que existe entre la retención temporal de imágenes de vigilancia por videocámara captadas con un equipo situado a la entrada de un banco y la creación de bancos de datos que

[22] Las autoridades de protección de datos danesa y sueca se manifestaron a favor de que las grabaciones de imágenes sólo pudieran almacenarse durante un breve período que no excediera los treinta días.

incluyan fotos y huellas dactilares facilitadas por los clientes del banco con su consentimiento, lo que supone una intrusión en mayor medida.

Por último, deberá prestarse atención a las decisiones que se tomen con respecto tanto a la *posible comunicación de los datos a terceras partes* (lo que, en principio, no deberá implicar a entidades que no estén relacionadas con las actividades de vigilancia p or videocámara) como a su *posible revelación, total o parcial, en el extranjero o, incluso, en la red* (también a la luz de las disposiciones relativas a la protección adecuada; véase el artículo 25 y siguientes de la Directiva).

Obviamente, el requisito según el cual las imágenes deberán ser pertinentes y no excesivas, también se refiere a la combinación de información procedente de diferentes responsables del tratamiento de sistemas de vigilancia por videocámara.

Las garantías mencionadas más arriba pretenden implantar, también de manera operacional, el principio al que se hace referencia en la normativa nacional de varios países: *el principio de moderación en el uso de datos personales* (cuyo objetivo consiste en evitar o reducir al mínimo posible el tratamiento de datos personales).

Este principio debería aplicarse en todos los sectores, teniendo en cuenta, también, el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales, o utilizando datos realmente anónimos, a pesar de que, inicialmente, pueda parecer necesario utilizar información personal.

Las consideraciones anteriores también son aplicables cuando se da la necesidad justificada de racionalizar los recursos comerciales [23] o de mejorar los servicios prestados a los usuarios[24].

F) Información a los interesados

La idoneidad y la naturaleza abierta de la utilización del equipo de vigilancia por videocámara implican el suministro de información adecuada a los interesados, con arreglo a los artículos 10 y 11 de la Directiva.

Los interesados serán informados con arreglo a los artículos 10 y 11 de la Directiva. Deberán estar al corriente de que la vigilancia por videocámara está en marcha, incluso cuando ésta esté relacionada con acontecimientos públicos y espectáculos o con actividades de publicidad (cámaras *web*); deberán ser informados de manera detallada sobre los lugares que se encuentran bajo control.

---

[23] Podría ser el caso, por ejemplo, para calcular la cantidad de cajas que deben mantenerse abiertas simultáneamente en un supermercado, en función del número de clientes que entren, o para trazar itinerarios de compra optimizados para los clientes de un supermercado.

[24] Para facilitar el acceso a un lugar de trabajo o a un medio de transporte específico para los que sea necesario realizar controles de identidad, puede ser suficiente con utilizar tarjetas con fotografía, si es posible en medios informáticos, sin necesidad de implantar un sistema de reconocimiento fisonómico.

No es necesario especificar la ubicación precisa del equipo de vigilancia; sin embargo, deberá quedar bien claro el contexto de la vigilancia.

La información deberá colocarse a una distancia razonable de los lugares controlados (a diferencia de lo ocurrido en algunos casos, en los que la colocación de las placas informativas a quinientos metros de las zonas vigiladas se ha considerado aceptable), incluso a la luz de las medidas tomadas para la grabación.

La información deberá estar a la vista y podrá suministrarse de manera resumida, a condición de que sea eficaz; podrá incluir símbolos que ya hayan resultado útiles en relación con la vigilancia por videocámara, así como indicaciones de prohibido fumar (lo que diferirá en función de si se graban o no imágenes). En todos los casos, deberá especificarse cuáles son los fines de la vigilancia por videocámara y quién es el responsable del tratamiento. El formato de la información deberá adaptarse a cada situación.

Sólo se permitirán restricciones específicas y bien fundadas a los requisitos informativos en los casos a los que se refieren los artículos 10, 11 y 13 de la Directiva (por ejemplo, podrá aplicarse una restricción temporal a los datos recogidos en el transcurso de investigaciones realizadas, en el marco de la Ley, por el abogado defensor, o con vistas a ejercer el derecho a la defensa, siempre y cuando la aportación de información pueda poner en peligro el logro de los fines específicos perseguidos).

Por último, se prestará especial atención al modo adecuado de facilitar la información a las personas invidentes.

G) Requisitos adicionales

En relación con estos requisitos adicionales, precauciones y garantías (tal y como se mencionan en la normativa sobre protección de datos y se resumen más arriba, en el punto 3), así como con relación a la necesidad de que el tratamiento de datos personales sea notificado a una autoridad independiente y esté sujeto a la supervisión de la misma con arreglo a los artículos 18, 19 y 28 de la Directiva, al Grupo le gustaría destacar, en concreto, las cuestiones siguientes:

a) Un número limitado de personas físicas, que deberá especificarse, estará autorizado a visualizar o acceder a las imágenes grabadas, cuando existan, exclusivamente para los fines perseguidos por la vigilancia por videocámara o con vistas al mantenimiento del equipo en cuestión, a fin de verificar su funcionamiento; por otra parte, esto puede ocurrir en base a una petición de acceso del interesado o una orden emitida por una autoridad policial o judicial con fines de investigación criminal.

   Siempre que la vigilancia por videocámara esté destinada únicamente a prevenir, detectar y controlar infracciones, la solución consistente en utilizar dos claves de acceso (una de las cuales estaría en posesión del responsable del tratamiento y la otra de la policía) podrá resultar útil para garantizar que las imágenes sólo las verá la policía, y no personal sin autorización (sin perjuicio de que el interesado ejerza su derecho legítimo de acceso a través de una solicitud presentada durante el breve período de retención de las imágenes).

b) Deberán aplicarse medidas de seguridad, a fin de evitar que se produzcan las eventualidades a las que se hace referencia en el artículo 17 de la Directiva, incluida la difusión de información que pudiera ser útil para proteger un derecho del interesado, a una tercera parte o al propio responsable del tratamiento (también con vistas a evitar la manipulación, la modificación o la destrucción de pruebas).

c) La calidad de las imágenes grabadas, cuando existan, también es fundamental (en concreto si se utilizan repetidamente los mismos medios de grabación, lo que implica el riesgo de no borrar completamente imágenes grabadas previamente).

d) Por último, es fundamental que los operadores implicados en las actividades de vigilancia por videocámara estén adecuadamente formados y al corriente de las medidas que deben tomar para cumplir plenamente los requisitos pertinentes.

H) Derechos del interesado

El carácter peculiar de los datos personales recogidos no impide que los interesados ejerzan los derechos a los que se hace referencia en los artículos 13 y 14 de la Directiva, prestando especial atención al derecho de oposición al tratamiento. De hecho, con arreglo a la Directiva 95/46, el interesado podrá oponerse, en cualquier momento, al tratamiento de datos que le conciernan[25] por razones legítimas propias de su situación particular.

El derecho del interesado al olvido y la usual brevedad del período de retención de las imágenes reducen el ámbito de aplicación del derecho del interesado a acceder a los datos personales que lo hacen identificable; no obstante, este derecho deberá protegerse especialmente en caso de que tenga lugar una petición detallada, como permitir la fácil recuperación de las imágenes pertinentes. Asimismo, deberá tenerse en cuenta la necesidad de proteger temporalmente los derechos de terceras partes.

Cualquier restricción basada en los esfuerzos necesarios para recuperar las imágenes, cuando dichos esfuerzos resulten claramente desproporcionados a causa de la brevedad del período de retención de las imágenes, se establecerá únicamente a través del Derecho derivado (véase el primer apartado del artículo 13 de la Directiva) y se prestará la debida atención al derecho del interesado a la defensa con respecto a acontecimientos específicos que puedan haber ocurrido en el período considerado.

I) Garantías adicionales relacionadas con operaciones de tratamiento específicas

[25] Excepto en los casos en los que la legislación nacional disponga lo contrario.

Se prohibirá la vigilancia por videocámara realizada exclusivamente a causa del origen racial de las personas, sus ideas políticas o religiosas , su pertenencia a sindicatos o sus hábitos sexuales (véase el artículo 8 de la Directiva).

Sin pretender establecer una lista exhaustiva de las diversas aplicaciones de la vigilancia por videocámara, el Grupo desea hacer hincapié en la necesidad de prestar más atención (en principio, cuando resulte apropiado, en el marco del control previo de las operaciones de tratamiento al que hace referencia el artículo 20 de la Directiva) a unos cuantos contextos en los que se recogen imágenes relativas a personas identificadas o identificables, ya que dichos contextos deberán evaluarse caso por caso.

Se hace referencia, en concreto, a los siguientes supuestos como resultado de experiencias o pruebas que ya están en marcha:

a) Interconexión permanente de sistemas de vigilancia por videocámara gestionados por diferentes responsables del tratamiento.
b) Posible asociación de imágenes y datos biométricos como huellas dactilares (por ejemplo, a la entrada de bancos).
c) Utilización de sistemas de identificación vocal.
d) Introducción, con arreglo a principios de proporcionalidad y en base a disposiciones específicas, de sistemas de indexación relativos a imágenes grabadas o sistemas de recuperación simultánea automática, en particular a través de datos de identificación.
e) Utilización de sistemas de reconocimiento fisonómico que no se limiten a la identificación de camuflajes de personas de paso, como barbas y pelucas falsas, sino que se basen en la localización de presuntos delincuentes, es decir, en la capacidad del sistema para identificar automáticamente a determinados individuos, a partir de plantillas o retratos robot que resulten de determinados rasgos externos (como el color de la piel o los ojos, la prominencia de los pómulos, etc.) o con arreglo a comportamientos anormales predefinidos (movimientos repentinos, paso por el mismo lugar incluso a intervalos determinados, manera de aparcar un vehículo, etc.). En este sentido, la intervención humana también es adecuada a la luz de los posibles errores que ocurran en tales casos, como se menciona más abajo, en el punto f).
f) Posibilidad de localizar, automáticamente, itinerarios y pistas, o de reconstruir o prever el comportamiento de una persona.
g) Toma de decisiones automatizadas basadas en el perfil de una persona o en análisis inteligentes y sistemas de intervención que no estén relacionados con señales de alarma estándar (como el hecho de entrar en un lugar sin la identificación necesaria o una alarma de incendio).

8. VIGILANCIA POR VIDEOCÁMARA EN EL CONTEXTO LABORAL

Este Grupo, ya en su «Dictamen nº 8/2001 sobre el tratamiento de datos personales en el contexto laboral», adoptado el 13 de septiembre de 2001, y en su «Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo», adoptado el 29 de mayo de 2002[26], puso de relieve, de manera más general, unos cuantos

[26] Ambos documentos están disponibles en la siguiente dirección:

principios destinados a proteger los derechos, las libertades y la dignidad de los interesados en el contexto laboral.

Además de las consideraciones realizadas en los documentos mencionados más arriba, en la medida en que sean realmente aplicables a la vigilancia por videocámara, conviene señalar que los sistemas de vigilancia por videocámara cuyo objetivo directo es controlar, desde una situación remota, la calidad y la cantidad de las actividades laborales y, por lo tanto, implican el tratamiento de datos personales en este contexto, por regla general no deberán estar permitidos.

La situación es diferente en lo que se refiere a los sistemas de vigilancia por videocámara que se utilizan, sujetos a las garantías adecuadas, para cumplir requisitos de producción y seguridad laboral, que también implican el control remoto (aunque sea indirectamente) [27].

La experiencia ha puesto de manifiesto, además, que la vigilancia no deberá abarcar lugares reservados al uso privado de los empleados o no estén destinados a la realización de tareas de trabajo (como servicios, duchas, vestuarios o zonas de descanso); que las imágenes recogidas exclusivamente para proteger la propiedad o detectar, evitar y controlar infracciones graves no deberán utilizarse para acusar a un empleado de una falta disciplinaria menor; y que deberá permitirse siempre a los empleados que utilicen para su defensa el contenido de las imágenes captadas.

Deberá facilitarse información a los empleados y a cualquier otra persona que trabaje en el lugar. Esta información incluirá la identidad del responsable del tratamiento y el objetivo de la vigilancia, así como otra información necesaria para garantizar que el tratamiento es justo en lo que respecta al interesado, por ejemplo en qué casos las grabaciones van a ser examinadas por la dirección de la empresa, el período de grabación y cuándo ésta se revelará a las autoridades judiciales. En el contexto laboral, la información facilitada en forma de símbolo, por ejemplo, no se considerará suficiente.

9. CONCLUSIÓN

El Grupo ha elaborado el presente documento de trabajo para contribuir a la aplicación uniforme de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE, en el ámbito de la vigilancia por videocámara.

* * *

En este contexto, también es fundamental que los Estados miembros aporten directrices relativas a la actividad de los productores, proveedores de servicios y

---

www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

[27] En estos casos, además de las consideraciones realizadas en el presente documento, deberá tenerse en cuenta también, de manera específica, la necesidad de respetar los derechos a los que se hace referencia en los acuerdos colectivos, que a veces se basan en la información colectiva de empleados o de sus sindicados correspondientes (es decir, aparte de la información que deberá facilitarse sobre la persona, de conformidad con las leyes de protección de datos); en otros casos, deberá firmarse un acuerdo previo con los representantes de los empleados o con los sindicatos en cuanto a la aplicación de medidas, también en lo que se refiere a la duración de la vigilancia y otras medidas relativas a la grabación. En algunos países, puede ser necesaria la intervención del Estado si las partes implicadas no se ponen de acuerdo.

distribuidores, e investigadores, con vistas al desarrollo de tecnologías, programas informáticos y dispositivos técnicos en consonancia con los principios a los que se hace referencia en el presente documento.

*** * ***

Hecho en Bruselas, el 25 de noviembre de 2002
Por el Grupo
El Presidente
Stefano RODOTA

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29

5401/01/ES/Final
WP 55

Documento de trabajo

relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo

Aprobado el 29 de mayo de 2002

Comentarios:

* los capítulos nacionales podrán modificarse posteriormente de acuerdo con las delegaciones nacionales

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: Dirección A (Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos) de la DG Mercado Interior de la Comisión Europea, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.

Sitio Internet: www.europa.eu.int/comm/privacy

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[1],

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 aprobado el siguiente documento de trabajo:

[1] Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm.

Documento de trabajo del Grupo de Trabajo «Artículo 29»[2] relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo

Proyecto de resumen

El presente documento de trabajo completa el dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral[3] y contribuye a la aplicación uniforme de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE relativa a la protección de datos[4]. No afecta a la aplicación de la legislación nacional en ámbitos vinculados a la protección de los datos.

El Grupo de Trabajo «Artículo 29» ha creado un subgrupo para examinar esta cuestión[5] y ha aprobado un **extenso documento,** disponible en Internet en la siguiente dirección[6]:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

En el presente documento de trabajo, el Grupo de Trabajo «Artículo 29» examina la cuestión de la vigilancia y el control de las comunicaciones electrónicas en el lugar de

---

[2] El Grupo de Trabajo «Artículo 29» es un grupo consultivo independiente compuesto por representantes de las autoridades de los Estados miembros encargadas de la protección de datos, cuya misión es, en particular, examinar todas las cuestiones relativas a la aplicación de las medidas nacionales adoptadas en virtud de la Directiva sobre protección de datos con el fin de contribuir a su aplicación uniforme.

[3] Dictamen adoptado el 13 de septiembre de 2001 y accesible en la siguiente dirección:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf .

Este dictamen incluye un análisis detallado de la aplicación de la Directiva relativa a la protección de datos (en particular, sus artículos 6, 7 y 8) al tratamiento de datos personales en el marco de las actividades profesionales.

[4] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23.11.95, p. 31.

[5] Al trabajo de este subgrupo han contribuido las siguientes autoridades de supervisión: AT, BE, DE, ES, FR, IR, IT, NL, UK.

[6] Este documento incluye un anexo en el que figura la legislación sobre protección de datos más pertinente de los Estados miembros con alguna repercusión en las actividades de vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo.

trabajo, o, dicho de otro modo, la vigilancia por el empleador de la utilización del correo electrónico e Internet por los trabajadores.

A la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, otros textos internacionales pertinentes y la Directiva 95/46/CE, el presente documento de trabajo ofrece una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empleador. Téngase en cuenta que en algunos Estados miembros la legislación puede prever un nivel de protección más elevado que el que contempla el presente documento de trabajo.

Los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. Estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores. Los casos en que el empleador es víctima de un delito imputable a un trabajador constituyen el ejemplo más claro.

No obstante, para equilibrar los distintos derechos e intereses es preciso tener en cuenta varios principios, en particular, el principio de proporcionalidad. Debe quedar claro que el mero hecho de que una actividad de control o vigilancia se considere útil para proteger el interés del empleador no justifica la intromisión en la vida privada del trabajador. Antes de aplicar en el lugar de trabajo cualquier medida de vigilancia, deben sopesarse una serie de aspectos que se detallan en el presente documento.

En las siguientes preguntas puede resumirse la naturaleza de esta evaluación:

a) ¿Es la actividad de vigilancia transparente para los trabajadores?

b) ¿Es necesaria? ¿No podría el empleador obtener el mismo resultado con métodos tradicionales de supervisión?

c) ¿Garantiza el tratamiento leal de los datos personales de los trabajadores?

d) ¿Es proporcional respecto a las preocupaciones que intenta solventar?

Al centrarse en la aplicación práctica de estos principios, el documento de trabajo proporciona orientación sobre el contenido mínimo de las directrices de las empresas en relación con la utilización del correo electrónico e Internet, que los empleadores y trabajadores pueden tomar como base para una adaptación posterior (habida cuenta de las especificidades de cada empresa, su tamaño y la legislación nacional en ámbitos vinculados a la protección de datos).

Al plantearse la utilización de Internet con fines privados, el Grupo de Trabajo «Artículo 29» considera que la **prevención debería prevalecer sobre la detección;** es decir, que es mejor para el empleador prevenir la utilización abusiva de Internet

que detectarla. En este contexto las soluciones tecnológicas pueden resultar especialmente útiles. Prohibir terminantemente que los trabajadores utilicen Internet con fines privados no parece razonable y no tiene en cuenta la ayuda que Internet puede aportarles en su vida diaria.

El Grupo de Trabajo desearía destacar que es esencial que el empleador informe al trabajador (i) de la presencia, utilización y objetivo de todo equipo y/o aparato de detección activado en su puesto de trabajo, así como (ii) de cualquier abuso de las comunicaciones electrónicas detectado (correo electrónico o Internet), salvo si existen razones imperiosas que justifiquen la continuación de la vigilancia encubierta[7], lo que normalmente no sucede. Puede transmitirse información rápida fácilmente mediante un programa informático, por ej. ventanas de advertencia que avisen al trabajador de que el sistema ha detectado y/o tomado medidas para evitar una utilización ilícita de la red.

Como recomendación práctica, los empleadores pueden considerar la posibilidad de proporcionar a los trabajadores dos cuentas de correo electrónico:

a) una de uso profesional exclusivo, en la que se permitiría un control dentro de los límites del presente documento de trabajo,

b) otra de uso estrictamente privado (o con autorización de utilizar el correo web), que sólo sería objeto de medidas de seguridad y que se controlaría para prevenir abusos en casos excepcionales.

El Grupo de Trabajo «Artículo 29» ha observado divergencias entre las legislaciones nacionales en ámbitos vinculados a la protección de datos, que se refieren principalmente a las excepciones previstas al derecho fundamental al secreto de correspondencia y al alcance y repercusión de la representación y la codecisión colectivas de los trabajadores. No obstante, no ha detectado divergencias entre las legislaciones nacionales en el ámbito de la protección de datos que puedan constituir obstáculos importantes para un enfoque común, por lo que ha redactado el presente documento de trabajo, que se revisará en 2002-2003 a la luz de la experiencia y la evolución en este ámbito.

[7] Los casos de vigilancia encubierta justificada constituyen un buen ejemplo.

1. LA VIGILANCIA EN EL LUGAR DE TRABAJO. UN RETO PARA LA SOCIEDAD.

Últimamente, la cuestión de la vigilancia de los trabajadores ha sido abordada en numerosas ocasiones por los medios de comunicación y es en la actualidad objeto de un debate público en la Comunidad. En efecto, la introducción progresiva en toda la Comunidad del correo electrónico en el lugar de trabajo ha sensibilizado tanto a los empleadores como a sus trabajadores de los riesgos de intromisión en su vida privada en el lugar de trabajo.

Al examinar la cuestión de la vigilancia, conviene tener siempre presente que, si bien los trabajadores tienen derecho a un cierto grado de respeto de la vida privada en el trabajo, este derecho no debe lesionar el derecho del empleador de controlar el funcionamiento de su empresa y de protegerse contra una actuación de los trabajadores susceptible de perjudicar sus intereses legítimos, por ejemplo la responsabilidad del empleador por acciones de sus trabajadores.

Aunque las nuevas tecnologías constituyen un desarrollo positivo de los recursos a disposición de los empleadores, las herramientas de vigilancia electrónica pueden utilizarse para atentar contra los derechos y libertades fundamentales de los trabajadores. Conviene no olvidar que, con la llegada de las tecnologías de la información, es vital que éstos se beneficien de los mismos derechos, ya trabajen en línea o fuera de línea.

Es necesario destacar también que las condiciones laborales han evolucionado, en el sentido de que en la actualidad cada vez es más difícil separar claramente el trabajo de la vida privada. En particular, a medida que se desarrolla la «oficina a domicilio», numerosos trabajadores continúan su trabajo en casa, utilizando la infraestructura informática puesta a su disposición por el empleador para estos u otros fines.

La dignidad humana de un trabajador prima sobre cualquier otra consideración. Al examinar esta cuestión, es importante tenerlo en cuenta, al igual que las consecuencias negativas que este tipo de acciones puede tener en la calidad de la relación de un trabajador con su empleador y en el trabajo propiamente dicho.

Habida cuenta de todos estos factores, no es de extrañar que esta problemática sea objeto de un intenso debate público; por ello es urgente contribuir a una interpretación uniforme de las disposiciones de la Directiva 95/46/CE y de las legislaciones nacionales que la aplican, a la luz de la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos.

El Grupo de Trabajo consideró por tanto que sería útil transmitir la información y las recomendaciones siguientes a los sectores público y privado. Es preciso señalar que el documento de trabajo cubre toda actividad vinculada a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, tanto la vigilancia en tiempo real como el acceso a datos almacenados.

2. INSTRUMENTOS JURÍDICOS INTERNACIONALES

2.1 ARTÍCULOS 8 Y 10 DEL CONVENIO EUROPEO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES.

Artículo 8

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Artículo 10

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o e para garantizar la autoridad y la imparcialidad del poder judicial.

Todos los Estados miembros y la Unión Europea deben cumplir las disposiciones del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Estos derechos se han ejercido tradicionalmente de forma vertical (es decir, el individuo frente al Estado) y actualmente se discute hasta qué punto pueden ejercerse horizontalmente (es decir, entre los individuos). No obstante, queda claro que en general estos derechos están presentes.

El Grupo de Trabajo considera por lo tanto que, a la hora de examinar las disposiciones nacionales adoptadas de conformidad con la Directiva 95/46/CE con el fin de contribuir a su aplicación uniforme, es preciso recordar los grandes principios consagrados por la jurisprudencia del Tribunal Europeo de Derechos Humanos en relación con esta disposición y, en particular, en lo que respecta al secreto de correspondencia.

En las sentencias dictadas hasta ahora, el Tribunal ha precisado que la protección de la «vida privada» consagrada por el artículo 8 no se limita al hogar, sino que se aplica también al lugar de trabajo.

El asunto **Niemitz contra Alemania** se refería al registro, por una autoridad pública, de la oficina del demandante. El Gobierno alemán alegó que el artículo 8 no ofrecía protección alguna contra el registro de una oficina, ya que el Convenio establece una clara distinción entre vida privada y domicilio, por una parte, y vida profesional y lugar de trabajo, por otra.

El Tribunal desestimó esta alegación y resolvió del siguiente modo:

«El respeto de la vida privada debe también englobar, hasta cierto punto, el derecho a entablar y desarrollar relaciones con los semejantes. ***Además, ninguna razón de principio permite excluir las actividades profesionales o comerciales del concepto de }vida privada~,*** *puesto que es en el trabajo donde la mayoría de las personas disponen de muchas, o incluso las máximas, oportunidades de relacionarse con el mundo exterior. Un hecho, destacado por la Comisión, lo confirma: no siempre se puede distinguir con claridad entre las actividades que pertenecen al ámbito profesional o laboral de las personas y las que no*[8]*».*

Más concretamente, en el asunto **Halford contra el Reino Unido**, el Tribunal estableció que la interceptación de las llamadas telefónicas efectuadas por los trabajadores desde su puesto de trabajo constituye una violación del artículo 8 del Convenio. Curiosamente, la Sra. Halford tenía a su disposición dos aparatos telefónicos, uno de los cuales estaba reservado para sus comunicaciones privadas. La utilización de estos teléfonos no estaba sometida a restricción alguna ni se le transmitió ninguna orientación a este respecto.

Para la Sra. Halford, la interceptación de sus llamadas telefónicas constituyó una violación del artículo 8 del Convenio. Su empleador, una autoridad pública, consideró en cambio que las llamadas telefónicas realizadas por la Sra. Halford desde su puesto de trabajo no estaban sujetas a la protección del artículo 8, ya que la demandante no podía confiar razonablemente en que se les reconociera carácter privado. En la vista ante el Tribunal, la defensa de la Administración declaró que el empleador debe en principio poder supervisar, sin que los interesados lo sepan de antemano, las llamadas que éstos realizan desde los aparatos que pone a su disposición.

Para el Tribunal, sin embargo, « *se desprende claramente de su jurisprudencia que las llamadas telefónicas que proceden de locales profesionales, al igual que las procedentes del domicilio, pueden incluirse en los conceptos de 'vida privada' y de 'correspondencia' citados en el apartado 1 del artículo 8 [...].*

No hay pruebas de que a la Sra. Halford se le hubiera avisado, en calidad de usuaria de la red interna de telecomunicaciones, de que las llamadas efectuadas mediante la misma podían ser interceptadas. El Tribunal considera que ella podía razonablemente esperar que se reconociera el carácter privado de este tipo de llamadas [...]»[9].

El concepto de «correspondencia» engloba no sólo las cartas redactadas en papel, sino también otras formas de comunicación electrónica recibidas o enviadas en el lugar de trabajo, como las llamadas telefónicas efectuadas o recibidas en locales profesionales o los

---

[8] 23 de noviembre de 1992, serie A n° 251/B, apartado 29; la negrita es añad ida.

[9] 27 de mayo de 1997.

mensajes electrónicos recibidos o enviados en ordenadores puestos a disposición en el lugar de trabajo.

Algunos interpretan la sentencia en el sentido de que parece implicar (aunque no se declare explícitamente) que si el empleador informa previamente al trabajador de que sus comunicaciones pueden interceptarse, el trabajador ya no podrá esperar que se reconozca carácter privado a sus llamadas, con lo que la interceptación no constituirá una violación del artículo 8 del Convenio. El Grupo de Trabajo opina que una advertencia previa al trabajador no basta para justificar una violación de sus derechos en cuanto a protección de datos.

De manera más general, de la jurisprudencia relativa al artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales pueden deducirse los tres principios siguientes:

a) Los trabajadores tienen confianza legítima en que se respetará su vida privada en el lugar de trabajo, confianza que no queda anulada por el hecho de utilizar herramientas de comunicación u otros medios profesionales del empleador.

   Sin embargo, el suministro de información adecuada por el empleador al trabajador puede disminuir esta confianza legítima.

b) El principio general del secreto de correspondencia se aplica a las comunicaciones en el lugar de trabajo, lo que incluye muy probablemente el correo electrónico y los ficheros anexos.

c) El respeto de la vida privada cubre también, hasta cierto punto, el derecho del individuo a entablar y desarrollar relaciones con sus semejantes. El hecho de que estas relaciones se produzcan en gran parte en el lugar de trabajo limita la necesidad legítima del empleador de aplicar medidas de vigilancia.

El artículo 10 es también pertinente, aunque en menor medida, puesto que regula las libertades de expresión e información y destaca el derecho del individuo a recibir y comunicar información e ideas sin injerencia de una autoridad pública. La pertinencia del artículo 10 parece reflejarse en las consideraciones del Tribunal en el asunto Niemitz contra Alemania previamente mencionado. Como afirmó el Tribunal, en el lugar de trabajo las personas desarrollan una parte importante de su relación con el mundo exterior y su derecho a la libertad de expresión desempeña indudablemente un papel en este contexto.

2.2 CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (STE N° 18)

Abierto a la firma el 28 de enero de 1981, el Convenio fue el primer instrumento internacional legalmente vinculante en el ámbito de la protección de datos. Este Convenio obliga a las partes a adoptar las medidas necesarias en su legislación nacional para aplicar los principios que enuncia con el fin de garantizar el respeto, en su territorio, de los derechos humanos fundamentales de todos los individuos con respecto al tratamiento de los datos de carácter personal[10].

---

[10] Véase también la Recomendación (89) 2 del Consejo de Europa sobre la protección de los datos de carácter personal utilizados con fines de empleo: http://cm.coe.int/ta/rec/1989/89r2.htm

Otros documentos importantes vinculados al Convenio 108, también pertinentes en este contexto, son los siguientes:

Recomendación (89) 2 del Consejo de Europa sobre la protección de los datos de carácter personal utilizados con fines de empleo [11].

Recomendación (97) 5 del Consejo de Europa sobre la protección de los datos médicos [12].

Recomendación (86) 1 del Consejo de Europa sobre la protección de los datos de carácter personal con fines de seguridad social [13].

Recomendación (95) 4 del Consejo de Europa sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, especialmente en lo que respecta a los servicios telefónicos.

2.3. LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Artículo 7. ***Respeto de la vida privada y familiar***

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8. ***Protección de datos de carácter personal***

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*

2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*

3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

La Carta de los Derechos Fundamentales de la Unión Europea parece ir en el mismo sentido que el Tribunal Europeo de Derechos Humanos. El concepto de secreto de correspondencia se ha ampliado para convertirse en un concepto de nueva generación: el «secreto de las comunicaciones», con el fin de reconocer a las comunicaciones electrónicas el mismo nivel de protección del que se beneficia el correo tradicional.

---

11 http://cm.coe.int/ta/rec/198 9 /89r2.htm .

12 http://cm.coe.int/ta/rec/1997/97r5.html

13 http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

Además, al conferir a la protección de datos una naturaleza claramente diferenciada, el artículo 8 completa la protección prevista por el artículo 7. Ello reviste una importancia singular en el contexto de la vigilancia del correo electrónico.

2.4. OFICINA INTERNACIONAL DEL TRABAJO (OIT)

Repertorio de recomendaciones prácticas de la Oficina Internacional del Trabajo sobre la protección de los datos personales de los trabajadores (1997).

«5. Principios generales

5.1. El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.

5.2. En principio, los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados.

5.3. Cuando los datos personales se exploten con fines distintos de aquéllos para los que fueron recabados, el empleador debería cerciorarse de que no se utilizan de un modo que sea incompatible con esa finalidad inicial y adoptar las medidas necesarias para evitar toda interpretación errada por causa de su aplicación en otro contexto.

5.4. Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores.

5.5. Las decisiones relativas a un trabajador no deberían basarse exclusivamente en un tratamiento informático de los datos personales que a él se refieran.

5.6. Los datos personales obtenidos por medios de vigilancia electrónica no deberían ser los únicos factores de evaluación profesional del trabajador. (...).

6.14. 1) Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos.

2) El secreto en materia de vigilancia sólo debería permitirse cuando

a) se realice de conformidad con la legislación nacional; o

b) existan sospechas suficientes de actividad delictiva u otras infracciones graves.

3) La vigilancia continua debería permitirse solamente si lo requieren la salud, la seguridad y la protección de los bienes. (...)

12.2. Los representantes de los trabajadores, cuando los haya, y de conformidad con la legislación y la práctica nacionales, deberían ser informados y consultados:

a) acerca de la instalación o modificación de sistemas automatizados de tratamiento de los datos personales de los trabajadores;

b) antes de la instalación de sistemas de vigilancia electrónica del comportamiento de los trabajadores en el lugar de trabajo; y

c) sobre la finalidad, el contenido, la aplicación y la interpretación de cuestionarios y pruebas relativos a los datos personales de los trabajadores.»

3. VIGILANCIA Y CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS EN EL LUGAR DE TRABAJO EN EL MARCO DE LA DIRECTIVA 95/46/CE

El presente documento de trabajo se basa en una aplicación de los principios enunciados en la Directiva 95/46/CE a la cuestión que nos ocupa, teniendo en cuenta el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que exige el respeto de la correspondencia y de la vida privada.

El empleador dispone de múltiples formas de vigilancia en el lugar de trabajo, cada una de las cuales con su propia problemática. El presente documento examinará dos formas de vigilancia, a las cuales se aplican principios similares: el control del correo electrónico y la vigilancia del acceso a Internet.

El punto de partida es la confirmación de la tesis defendida en el dictamen 8/2001 según el cual la Directiva 95/46/CE se aplica al tratamiento de los datos personales en el contexto profesional como en cualquier otro contexto[14]. Además de la Directiva general 95/46/CE, la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones puede también resultar pertinente. Esta Directiva especifica y completa la Directiva 95/46/CE respecto al tratamiento de los datos personales en el sector de las telecomunicaciones. Además de estar prevista en la Directiva 95/46/CE, la vigilancia por el empleador de las comunicaciones electrónicas, incluidos el correo electrónico y el acceso a Internet, podría también entrar en el ámbito de aplicación de la Directiva 97/66/CE, que actualmente se está examinando en el contexto de la revisión del marco jurídico comunitario en materia de telecomunicaciones. Cuando esta Directiva es aplicable, sus artículos 5 (Confidencialidad de las telecomunicaciones) y 6 (Tráfico y facturación) pueden desempeñar un papel especialmente importante.

3.1 PRINCIPIOS GENERALES APLICABLES A LA VIGILANCIA DEL CORREO ELECTRÓNICO Y LA UTILIZACIÓN DE INTERNET

Los siguientes principios de protección de datos se derivan de la Directiva 95/46/CE y deben respetarse en el tratamiento de los datos personales que implica este tipo de vigilancia. Para que una actividad de control sea legal y se justifique, deben respetarse todos los principios siguientes.

3.1.1. NECESIDAD

Según este principio, el empleador, antes de proceder a este tipo de actividad, debe comprobar si una forma cualquiera de vigilancia es absolutamente necesaria para un objetivo específico. Debería plantearse la posibilidad de utilizar métodos tradicionales de supervisión, que implican una intromisión menor en la vida privada de los trabajadores, y, cuando proceda, aplicarlos antes de recurrir a una forma de vigilancia de las comunicaciones electrónicas.

---

[14] http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48fr.pdf

Sólo en circunstancias excepcionales se considerará necesaria la vigilancia del correo electrónico o de la utilización de Internet de un trabajador. Podría resultar necesario controlar el correo electrónico de un trabajador para obtener una confirmación o una prueba de determinados actos del mismo. En este tipo de actos se incluiría la actividad delictiva de un trabajador que obligara al empleador a defender sus intereses, por ejemplo, cuando es responsable subsidiario de los actos del trabajador. Estas actividades de vigilancia incluirían también la detección de virus y, en general, cualquier actividad realizada por el empleador para garantizar la seguridad del sistema.

Cabe mencionar que la apertura del correo electrónico de un trabajador puede también resultar necesaria por razones distintas del control o la vigilancia, por ejemplo para mantener la correspondencia cuando el trabajador está ausente (por ej. enfermedad o vacaciones) o cuando la correspondencia no puede garantizarse de otra forma (por ej. mediante las funciones de respuesta o desviación automática).

El principio de necesidad significa también que un empleador sólo debe conservar los datos durante el tiempo necesario para el objetivo específico de la actividad de vigilancia.

3.1.2. FINALIDAD

Este principio significa que los datos deben recogerse con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines. En el presente contexto, el principio de «compatibilidad» significa, por ejemplo, que si el tratamiento de los datos se justifica a efectos de seguridad del sistema, estos datos no podrán tratarse posteriormente con otro objetivo, por ejemplo, para supervisar el comportamiento del trabajador.

3.1.3. TRANSPARENCIA

Este principio significa que un empleador debe indicar de forma clara y abierta sus actividades. Dicho de otro modo, el control secreto del correo electrónico por el empleador está prohibido, excepto en los casos en que exista en el Estado miembro una ley que lo autorice en virtud del artículo 13 de la Directiva [15]. Ello puede ocurrir cuando se detecte una actividad delictiva particular (que haga necesaria la obtención de pruebas, y siempre que se cumplan las normas jurídicas y procesales de los Estados miembros) o cuando existan leyes nacionales que autoricen al empleador, previendo las garantías necesarias, a adoptar algunas medidas para detectar infracciones en el lugar de trabajo.

Por otra parte, este principio puede subdividirse en tres aspectos:

3.1.3.1. LA OBLIGACIÓN DE PROPORCIONAR INFORMACIÓN AL INTERESADO

Se trata probablemente del ejemplo más pertinente del principio de transparencia aplicado a la cuestión que nos ocupa. Significa que el empleador debe transmitir a

---

[15] El artículo 13 de la Directiva permite a los Estados m iembros adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en algunos artículos de dicha Directiva, cuando tal limitación constituya una medida necesaria para la salvaguardia de intereses públicos importantes, como la seguridad del Estado, o la prevención, la investigación, la detección y la represión de infracciones penales, o también la protección del interesado o de los derechos y libertades de otras personas.

su personal una declaración clara, precisa y fácilmente accesible de su política relativa a la vigilancia del correo electrónico y la utilización de Internet.

Los trabajadores deben ser informados de manera completa sobre las circunstancias particulares que pueden justificar esta medida excepcional; así como del alcance y el ámbito de aplicación de este control. Esta información debería incluir:

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empl eador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

El Grupo de Trabajo desearía destacar aquí que es aconsejable desde un punto de vista práctico que el empleador informe inmediatamente al trabajador de cualquier abuso de las comunicaciones electrónicas detectado, salvo si razones imperiosas justifican la continuación de la vigilancia [16], lo que normalmente no es el caso. Puede transmitirse información rápida fácilmente mediante un programa informático, por ej. ventanas de advertencia que avisen al trabajador de que el sistema ha detectado una utilización ilícita de la red. Un gran número de malentendidos podrían también evitarse de esta manera.

Otro ejemplo del principio de transparencia es la práctica de los empleadores consistente en informar y/o consultar a los representantes de los trabajadores antes de introducir políticas que les conciernan. Cabe destacar que las decisiones relativas a la vigilancia de los trabajadores, en particular, el control de sus comunicaciones electrónicas, están cubiertas por la reciente Directiva 2002/14/CE, siempre que la empresa en cuestión figure en su ámbito de aplicación. En particular, esta Directiva establece la necesidad de informar y consultar a los trabajadores sobre decisiones que puedan implicar cambios importantes en la organización del trabajo o en las relaciones contractuales. La legislación nacional o los convenios colectivos pueden introducir disposiciones más favorables incluso para los trabajadores.

---

[16] En tales casos, por ejemplo, estaría justificada l a vigilancia encubierta.

Es posible que los convenios colectivos no sólo obliguen al empleador a informar y consultar a los representantes de los trabajadores antes de instalar sistemas de vigilancia, sino que también supediten esta instalación a su consentimiento previo.

Asimismo, en los convenios colectivos pueden establecerse los límites de la utilización de Internet y del correo electrónico por los trabajadores, así como proporcionarse información detallada sobre el control de esta utilización.

3.1.3.2. LA OBLIGACIÓN DE NOTIFICAR A LAS AUTORIDADES DE SUPERVISIÓN ANTES DE LA APLICACIÓN DE UN TRATAMIENTO TOTAL O PARCIALMENTE AUTOMATIZADO O DE UN CONJUNTO DE TRATAMIENTOS DE ESTE TIPO

Se trata de otro medio de garantizar la transparencia, ya que los trabajadores pueden siempre comprobar en los registros de protección de datos, por ejemplo, qué categorías de datos personales de los trabajadores puede procesar el empleador, con qué finalidad y para qué destinatarios.

3.1.3.3. EL DERECHO DE ACCESO

Un trabajador, así como cualquier otra persona de conformidad con la Directiva [17], tiene derecho a acceder a los datos personales que le conciernen tratados por su empleador y, cuando proceda, a pedir la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular, debido a su carácter incompleto o inexacto.

El acceso de los trabajadores a los archivos del empleador sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos es una herramienta poderosa que los trabajadores pueden utilizar individualmente para garantizar la

---

[17] Artículo 12: Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

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

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

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

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

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

lealtad y legitimidad de las actividades de vigilancia en el lugar de trabajo. El acceso a los archivos del empleador puede no obstante resultar problemático en circunstancias excepcionales, por ejemplo, el acceso a los datos considerados de evaluación.

El Grupo de Trabajo ya abordó de forma somera esta cuestión[18] y podría proporcionar más orientaciones al respecto a la luz de la experiencia.

3.1.4. LEGITIMIDAD

Este principio significa que una operación de tratamiento de datos sólo puede efectuarse si su finalidad es legítima según lo dispuesto en el artículo 7 de la Directiva y la legislación nacional de transposición. La letra f) del artículo 7 de la Directiva se aplica especialmente a este principio, dado que, para autorizarse en virtud de la Directiva 95/46/CE, el tratamiento de los datos de un trabajador debe ser necesario para la satisfacción del interés legítimo perseguido por el empleador y no perjudicar los derechos fundamentales de los trabajadores.

La necesidad del empleador de proteger su empresa de amenazas importantes, por ejemplo para evitar la transmisión de información confidencial a un competidor, puede considerarse un interés legítimo.

El tratamiento de datos delicados en este contexto es especialmente problemático, ya que el artículo 8 de la Directiva no prevé un equilibrio de intereses según lo dispuesto en la letra f) del artículo 7 de la Directiva. Sin embargo, la letra b) del apartado 2 del artículo 8 hace referencia al tratamiento «necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas».

El tratamiento de datos delicados en relación con las actividades de control y vigilancia es una cuestión espinosa que no sólo es pertinente en un contexto profesional. Se trata en efecto de una cuestión de carácter general sobre la cual el Grupo podría proporcionar orientación en el futuro.

En realidad, a menos que la legislación nacional las autorice específicamente previendo garantías adecuadas, las actividades de vigilancia destinadas directamente al tratamiento de datos delicados relativos a los trabajadores no son legítimas de conformidad con la Directiva 95/46/CE ni tampoco aceptables. No obstante, tampoco parece aceptable impedir o complicar en exceso las actividades de vigilancia (que, en muchos casos no sólo son legales, sino también deseables, como las que tienen por objeto directamente garantizar la seguridad del sistema) por el mero hecho de que sea inevitable el tratamiento de información delicada.

3.1.5. PROPORCIONALIDAD

Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa.

---

[18] Véase la recomendación 1/2001 sobre los datos de evaluación de los trabajadores.

El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua).

Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empleador. Si el acceso al contenido de los mensajes es indispensable, convendría tener en cuenta el respeto de la vida privada de los destinatarios externos e internos de la organización. Por ejemplo, el empleador no puede obtener el consentimiento de las personas ajenas a la organización que envían mensajes a los miembros de su personal. Del mismo modo, el empleador debería aplicar todos los medios razonables para informar a las personas ajenas a la organización de la existencia de actividades de vigilancia que pudieran afectarlas. Se podría, por ejemplo, insertar avisos de la existencia de sistemas de vigilancia en todos los mensajes salientes de la organización.

La tecnología ofrece al empleador importantes posibilidades de evaluar la utilización del correo electrónico por sus trabajadores, comprobando, por ejemplo, el número de mensajes enviados y recibidos o el formato de los documentos adjuntos; por ello la apertura efectiva de los mensajes electrónicos es desproporcionada. La tecnología puede también utilizarse para garantizar que sean proporcionadas las medidas adoptadas por el empleador para proteger de todo abuso el acceso a Internet autorizado a su personal, utilizando mecanismos de bloqueo más que de vigilancia [19].

Deberían crearse sistemas de tratamiento de las comunicaciones electrónicas para limitar al mínimo estricto la cantidad de datos personales tratados [20].

Por lo que se refiere a la cuestión de la proporcionalidad, debe destacarse que el mecanismo de negociación colectiva puede resultar muy útil para decidir qué acciones son proporcionadas al riesgo que corre el empleador. Es posible alcanzar un acuerdo entre el empleador y los trabajadores sobre la forma de conciliar los intereses de ambas partes.

3.1.6. EXACTITUD Y CONSERVACIÓN DE LOS DATOS

---

[19] Ya existen numerosos ejemplos prácticos de la utilización de estos medios te cnológicos:

- Internet: algunas empresas utilizan un programa informático que puede configurarse para impedir la conexión a categorías predeterminadas de sitios web. Tras consultar la lista global de los sitios web visitados por su personal, el empleador puede decidir añadir algunos sitios a la lista de los bloqueados (eventualmente después de haber informado a los trabajadores de que se bloqueará la conexión con este sitio, salvo si un trabajador le demuestra la necesidad de conectarse).

- Correo electrónico: otras empresas utilizan una función de desviación automática hacia un servidor aislado para todos los mensajes que superan un determinado volumen. Se informa automáticamente al destinatario de que se ha desviado un mensaje sospechoso hacia este servidor, donde puede consultarlo.

[20] Proyecto de Directiva 97/66, considerando 30.

Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios enunciados en este capítulo) que incluyan datos procedentes de una cuenta de correo electrónico de un trabajador, de su utilización de Internet o relativos a las mismas deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. Los empleadores deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales. Normalmente, es difícil imaginar que pueda justificarse un período de conservación superior a tres meses.

3.1.7. SEGURIDAD

Este principio obliga al empleador a aplicar las medidas técnicas y organizativas adecuadas para proteger todos los datos personales en su poder de toda intromisión exterior. Incluye también el derecho del empleador a proteger su sistema contra los virus y puede implicar el análisis automatizado de los mensajes electrónicos y de los datos relativos al tráfico en la red.

El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, siempre y cuando existan garantías adecuadas. Por ejemplo, los empleadores pueden ahora utilizar tecnologías que responden a sus intereses en términos de seguridad, pero que no violan el derecho de los trabajadores a la vida privada.

El Grupo de Trabajo «Artículo 29» llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder.

4. CONTROL DEL CORREO ELECTRÓNICO

4.1. EL SECRETO DE CORRESPONDENCIA

Tal como se ha explicado anteriormente en el presente documento de trabajo, el Grupo de Trabajo considera que las situaciones en línea y fuera de línea no deben tratarse de manera diferente sin motivo y que, por lo tanto, los mensajes electrónicos deben beneficiarse de la misma protección de los derechos fundamentales que el correo tradicional [21]. La jurisprudencia del Tribunal Europeo de Derechos Humanos ha proporcionado orientación sobre la aplicación del principio del secreto de correspondencia en una sociedad democrática. No obstante, los ordenamientos jurídicos de los Estados miembros interpretan este principio de manera ligeramente diferente, en particular, desde el punto de vista de su ámbito de aplicación a las comunicaciones profesionales, tanto por lo que se refiere a su contenido como a los datos relativos al tráfico. Desde el punto de vista de la protección de datos, este principio tiene consecuencias importantes al considerar el grado de intromisión tolerable en el correo electrónico de los trabajadores.

El Grupo de Trabajo «Artículo 29» opina que las comunicaciones electrónicas que proceden de locales profesionales pueden estar cubiertas por los conceptos de «vida privada» y de «correspondencia» según lo dispuesto en el apartado 1 del artículo 8 del Convenio europeo. Hay poco margen de interpretación a este respecto, puesto que el Tribunal ya reguló claramente la cuestión en el asunto **Halford contra el Reino Unido mencionado más arriba.**

Lo que queda por examinar, y se presta de hecho a cierto margen de interpretación, es en qué medida pueden permitirse excepciones o restricciones a este principio, sobre todo cuando entra en conflicto con derechos y libertades de otros que también son protegidos por el Convenio (por ej. los intereses legítimos del empleador). **En cualquier caso, el secreto de las comunicaciones y de la correspondencia no depende de la ubicación y la propiedad de los medios electrónicos utilizados, según se establece en constituciones y principios jurídicos fundamentales.**

El Grupo de Trabajo «Artículo 29» desearía, sin embargo, recordar que no se trata de un problema específico del tratamiento de los datos de carácter personal en el contexto profesional, sino de un problema general que se deriva del hecho de que las legislaciones y reglamentos sobre protección de datos no se aplican en abstracto. Se supone que los derechos relativos a la protección de datos se aplican a distintos sistemas jurídicos, con otras leyes vigentes que prevén otros derechos y obligaciones para los individuos (por ej.

---

[21] Una de las primeras recomendaciones formuladas por el Grupo de Trabajo, la Recomendación 3/97 «Anonimato en Internet», ya precisaba que las situaciones en línea y fuera de línea debían tratarse de manera idéntica.

Véase http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6es.pdf

El documento del Grupo de Trabajo sobre Internet, que es el más importante adoptado por el Grupo de Trabajo sobre la privacidad en Internet, hacía hincapié en esta idea en su capítulo 3, página 23:

Véase http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37es.pdf

el Derecho laboral). No obstante, el Grupo de Trabajo «Artículo 29» está convencido de que las soluciones propuestas en el presente documento pueden ser útiles para alcanzar este difícil equilibrio de intereses.

4.2. LEGITIMACIÓN DE CONFORMIDAD CON LA DIRECTIVA 95/46/CE

Los mensajes electrónicos contienen datos personales que son protegidos por la Directiva 95/46/CE, por lo que los empleadores deben tener un motivo legítimo para proceder al tratamiento de estos datos. Como se explicó de manera detallada en el dictamen 8/2001, los trabajadores deben dar su consentimiento libremente y con conocimiento de causa; y los empleadores no deben recurrir al consentimiento como medio general de legitimar tratamientos de este tipo.

La legitimación más idónea de la vigilancia del correo electrónico puede encontrarse en la letra f) del artículo 7 de la Directiva, que prevé que el tratamiento sólo pueda efectuarse 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. Antes de analizar la aplicación de esta disposición al ámbito que nos ocupa, conviene indicar que tal legitimación no puede anular derechos y libertades fundamentales de los trabajadores. Ello incluye, en su caso, el derecho fundamental al secreto de la correspondencia.

El Grupo de Trabajo ya ha opinado lo siguiente [22]:

«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.»

Dado que los mensajes electrónicos contienen datos personales que se refieren tanto al emisor como al destinatario y que los empleadores pueden en general obtener el consentimiento de una de estas partes sin demasiadas dificultades (a menos que el correo electrónico incluya también la correspondencia entre trabajadores de la empresa), la posibilidad de legitimar el control del correo electrónico sobre la base del consentimiento es muy limitada. Estas consideraciones se aplican también a la letra b) del artículo 7 de la Directiva, ya que una de las partes de la correspondencia nunca tendría contrato con el responsable del tratamiento con arreglo a dicha disposición, es decir, para el control de la correspondencia.

En esta fase, debe señalarse que cuando el trabajador recibe una cuenta de correo electrónico para uso estrictamente personal o puede acceder a una cuenta de correo web, la apertura por el empleador de los mensajes electrónicos de esta cuenta (excepto para detectar virus) sólo podrá justificarse en circunstancias muy limitadas [23] y no podrá justificarse en circunstancias normales con arreglo a la letra f) del artículo 7, ya que acceder a este tipo de datos no es necesario para satisfacer un interés legítimo del

---

[22] Véase el recuadro de la página 23 del dictamen 8/2001.

[23] Por ejemplo, actividades delictivas del trabajador que obliguen al empleador a defender sus intereses, cuando sea responsable de los actos del trabajador o cuando él mismo sea víctima del delito.

empleador. En este caso, prevalece por el contrario el derecho fundamental al secreto de correspondencia.

En consecuencia, la cuestión de en qué medida la letra f) del artículo 7 autoriza el control del correo electrónico depende de la aplicación caso por caso de los principios fundamentales explicados en el capítulo 3.2. Como ya se menciona en el apartado 3.1.4 (Legitimidad), al sopesar los intereses de las partes, conviene tener en cuenta el respeto de la vida privada de las personas ajenas a la organización afectadas por la actividad de vigilancia.

4.3 INFORMACIÓN MÍNIMA RECOMENDADA QUE UNA EMPRESA DEBERÍA FACILITAR A SU PERSONAL

Al elaborar su política, los empleadores deben respetar los principios enunciados en el apartado 3.1.3 relativo al principio general de transparencia[24], habida cuenta de las necesidades y el tamaño de la organización.

Además, en el ámbito más específico del correo electrónico, deberán abordarse los puntos siguientes:

a) Determinar si un trabajador está autorizado a disponer de una cuenta de correo electrónico de uso estrictamente personal, si está permitida la utilización de cuentas de correo web en el lugar de trabajo y si el empleador recomienda a su personal la utilización de una cuenta privada de correo web para utilizar el correo electrónico con fines exclusivamente personales (véase el capítulo 4.4).

b) Los acuerdos con los trabajadores sobre el acceso al contenido del correo electrónico, por ej. cuando el trabajador se ausenta repentinamente, y las finalidades específicas de este acceso.

c) Indicar el periodo de conservación de las posibles copias de protección de los mensajes.

d) Precisar cuándo se borran definitivamente los mensajes electrónicos del servidor.

e) Cuestiones de seguridad.

24

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia ado ptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

f) Participación de los representantes de los trabajadores en la formulación de la política.

Conviene señalar que el empleador debe garantizar permanentemente la actualización de su política de acuerdo con la evolución tecnológica y la opinión de su personal.

4.4 CORREO WEB[25]

El Grupo de Trabajo considera que la posibilidad de que los trabajadores utilicen una cuenta privada de correo electrónico o un correo web podría suponer una solución pragmática del problema. Una recomendación en este sentido por parte del empleador facilitaría la distinción entre el correo electrónico de uso profesional y el de uso privado y reduciría el riesgo de intromisión de los empleadores en la vida privada de sus trabajadores. Además, los costes suplementarios para el empleador serían nulos o mínimos.

Si se adopta esta política, el empleador podrá controlar, en casos específicos en que existan sospechas graves sobre el comportamiento de un trabajador, en qué medida éste utiliza su ordenador con fines personales, contabilizando el tiempo que emplea en las cuentas del correo web. Esta solución satisface los intereses del empleador y evita el riesgo de revelación de datos personales de los trabajadores, y, en particular, de datos delicados.

Además esta política favorecería también a los trabajadores, porque les permitiría saber con seguridad el nivel de confidencialidad que pueden esperar, lo que no quizá no sería el caso con códigos de conducta más complejos y confusos. Dicho esto, conviene también indicar lo siguiente:

a) **El hecho de autorizar la utilización del correo web o de cuentas privadas no es óbice para la plena aplicación de los puntos anteriores del presente capítulo a otras cuentas de correo electrónico en el lugar de trabajo.**

b) Al autorizar el correo web, las empresas deben saber que su uso puede comprometer la seguridad de sus redes, en particular, por lo que se refiere a la proliferación de virus.

c) Los trabajadores deberían saber que, a veces, los servidores del correo web están situados en terceros países que quizá no cuenten con un sistema adecuado de protección de los datos de carácter personal.

Debe tenerse en cuenta que estas consideraciones se aplican a las relaciones normales entre empleadores y trabajadores. Podría resultar necesario aplicar normas especiales a la comunicación de los trabajadores obligados a guardar secreto profesional.

---

[25] El correo web es un sistema de correo electrónico en la red que ofrece funciones de correo electrónico a partir de cualquier distribuidor POP o IMAP y que está protegido generalmente por un nombre de usuario y una contraseña.

5. CONTROL DEL ACCESO A INTERNET

5.1 UTILIZACIÓN DE INTERNET CON FINES PRIVADOS EN EL LUGAR DE TRABAJO

En primer lugar, conviene destacar que incumbe a la empresa decidir si autoriza a su personal a navegar en Internet con fines privados y, en caso afirmativo, en qué medida se tolera esta utilización privada.

El Grupo considera no obstante que una prohibición absoluta de la utilización de Internet con fines privados por los trabajadores podría considerarse inaplicable y un tanto irrealista, ya que no se tendría en cuenta el apoyo que Internet puede brindar a los trabajadores en su vida diaria.

5.2. PRINCIPIOS RELATIVOS AL CONTROL DE LA UTILIZACIÓN DE INTERNET

Al considerar la cuestión del control de la utilización de Internet por los trabajadores pueden aplicarse algunos principios.

En la medida de lo posible, **la prevención debería primar sobre la detección**. En otras palabras, al empleador le es más beneficioso prevenir la utilización abusiva de Internet por medios técnicos que destinar recursos a su detección. Dentro del límite de lo que es razonablemente posible, la política de la empresa respecto a Internet debería basarse en herramientas técnicas para limitar el acceso, más que en dispositivos de control de los comportamientos, por ejemplo, bloqueando el acceso a algunos sitios o instalando advertencias automáticas.

El suministro al trabajador de información rápida sobre la detección de una utilización sospechosa de Internet es importante para minimizar los problemas. Aunque sea necesaria, toda medida de control debe ser **proporcionada** al riesgo que corre el empleador. En la mayoría de los casos, la utilización abusiva de Internet puede detectarse sin tener que analizar el contenido de los sitios visitados. Por ejemplo, la comprobación del tiempo empleado o la elaboración de una lista de los sitios más visitados por un servicio podría bastar para confirmar al empleador que sus sistemas se emplean correctamente. Si estas comprobaciones generales revelaran una posible utilización abusiva de Internet, el empleador podría entonces considerar la posibilidad de proceder a nuevos controles en la zona de riesgo.

Al analizar la utilización de Internet por los trabajadores, los empleadores **deberían evitar sacar conclusiones precipitadas**, dada la facilidad con que pueden visitarse involuntariamente algunos sitios a través de respuestas de motores de búsqueda, vínculos hipertextuales ambiguos, pancartas publicitarias engañosas o errores al pulsar las teclas. En todos los casos, deberán presentarse al trabajador en cuestión todos los hechos de que se le acusa y ofrecerle la posibilidad de refutar la utilización abusiva alegada por el empleador.

5.3 CONTENIDO MÍNIMO RECOMENDADO DE LA POLÍTICA DE LA EMPRESA SOBRE LA UTILIZACIÓN DE INTERNET

1. La información que se especifica en el apartado 3.1.3., relativo al principio de transparencia[26].

   Además, en el ámbito más específico del correo electrónico, deberán abordarse los puntos siguientes.

2. El empleador deberá precisar claramente a los trabajadores en qué condiciones se autoriza la utilización de Internet con fines privados e indicarles los elementos que no pueden visualizar o copiar. Estas condiciones y restricciones deberán explicarse al personal.

3. Deberá informarse a los trabajadores de los sistemas instalados para impedir el acceso a algunos sitios o para detectar una posible utilización abusiva. Deberán precisarse el alcance del control, por ejemplo si este control se efectúa de manera individualizada o por departamentos de la empresa, o si el contenido de los sitios consultados será visualizado o registrado por el empleador en determinados casos. Además, la política de la empresa deberá especificar, cuando proceda, el uso que se hará de los datos recogidos sobre las personas que visitaron sitios específicos.

4. Deberá informarse a los trabajadores del papel de sus representantes, tanto en la aplicación de la política como en la investigación de las presuntas infracciones.

CONCLUSIÓN

El Grupo de Trabajo ha redactado el presente documento de trabajo con el fin de contribuir a la aplicación uniforme de las medidas nacionales adoptadas de conformidad con la Directiva 95/46/CE en el ámbito de la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo. (Sírvanse consultar los resúmenes de las legislaciones nacionales que se adjuntan al presente documento).

El Grupo de Trabajo ha observado algunas divergencias entre las legislaciones nacionales, principalmente en ámbitos vinculados a la protección de datos que tratan de las excepciones al derecho fundamental al secreto de correspondencia y al alcance y repercusiones de la representación y la codecisión colectivas. Desearía, sin embargo, destacar que ninguna divergencia entre las legislaciones de los Estados miembros que

---

26

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

aplican la Directiva 95/46/CE constituye un obstáculo fundamental para la adopción del enfoque común previsto en los principios y buenas prácticas señaladas en el presente documento de trabajo.

El Subgrupo de Empleo seguirá revisando el presente documento de trabajo a la luz de la experiencia y de futuros avances en este ámbito durante 2002- 2003.

Hecho en Bruselas, el 29 de mayo de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

5035/01/ES/Final
WP 56

Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE

Aprobado el 30 de mayo de 2002

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. Protección de Datos. B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.
Dirección Internet: www.europa.eu.int/comm/privacy

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[1],

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 aprobado el siguiente documento de trabajo:

1. Introducción

El objetivo del presente documento es debatir la cuestión de la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento, en particular, la recogida, de datos personales por sitios web establecidos fuera de la Unión Europea[2]. El presente documento pretende servir de herramienta y punto de referencia para los responsables del tratamiento y sus asesores en el examen de los casos que implican el tratamiento de datos de carácter personal en Internet por sitios web establecidos fuera de la Unión Europea. Debido a la gran complejidad de este ámbito y al dinamismo del entorno Internet, este documento no propone soluciones definitivas que puedan aplicarse a todos los casos posibles relacionados con la cuestión.

En su documento de trabajo «Privacidad en Internet»[3], el Grupo de Trabajo sobre protección de datos «Artículo 29» señaló la necesidad evidente de especificar la aplicación concreta de la norma relativa a la legislación aplicable de la Directiva general de protección de datos (letra c) del apartado 1 del artículo 4)[4], en particular para el tratamiento en línea de datos personales por una persona establecida fuera del territorio comunitario. Regularmente se invita a las autoridades nacionales de control de la protección de datos a asesorar sobre esta cuestión a empresas y particulares.

La necesidad de determinar si el Derecho nacional se aplica a las situaciones en las que intervienen varios países no es específica de la protección de datos, ni de Internet, ni de la Unión Europea. Se trata de una cuestión general de Derecho internacional que se plantea en situaciones en línea y fuera de línea, cuando intervienen uno o más elementos que afectan a más de un país. Es necesario decidir sobre la legislación aplicable para poder desarrollar una solución sobre el fondo.

---

1 Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 La Directiva 95/46/CE relativa a la protección de datos se aplica también en el Espacio Económico Europeo (EEE). La referencia a la Unión Europea en el presente documento debe entenderse como una referencia al EEE.

3 «Privacidad en Internet:- Enfoque comunitario integrado de la protección de datos en línea -», WP 37, 21 de noviembre de 2000.

4 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23 de noviembre de 1995, pp. 31 a 50, disponible en la siguiente dirección: http://europa.eu.int/eur-lex/es/lif/dat/1995/es_395L0046.html.

Estas decisiones implican el examen de una serie de factores. En primer lugar, un Estado debe proteger los derechos e intereses de sus ciudadanos, residentes, industrias y demás instancias reconocidas por el Derecho nacional. En numerosos países, el Derecho Penal (que es lo contrario de las leyes que conceden derechos y libertades) exige la aplicación más amplia con efectos a nivel internacional. Asuntos famosos, como los de Yahoo! [5] o CompuServe[6], muestran cómo aplican los tribunales el Derecho Penal nacional para prohibir el acceso a contenidos pornográficos o racistas en servidores de Internet extranjeros. Una decisión reciente del Tribunal Supremo alemán (sala de lo penal) condenó a un editor del «Auschwitz Lüge» (negación de la existencia de Auschwitz) en un sitio web australiano a pesar de que no se demostró que se había accedido a este sitio desde Alemania [7]. Según el Tribunal, en el contexto de este delito particular es suficiente que el contenido en Internet «pueda» tener un efecto negativo en el orden público en Alemania y no es necesario que el hecho se haya producido efectivamente.

Esta aplicación internacional de normas protectoras expresa en general el deseo del legislador o el juez de proteger a los ciudadanos cuando la situación lo exige, pese a las dificultades intrínsecas de la aplicación en una situación de carácter transfronterizo, y de aplicar estas normas en la práctica con el fin de garantizar que se alcanza el objetivo perseguido.

En la legislación comunitaria, varios ejemplos ilustran esta búsqueda de coherencia.

En el ámbito del Derecho de la competencia, la Comisión Europea puede tomar decisiones que afecten a sociedades establecidas fuera de la UE si operan en el territorio de la Unión. Como ejemplo, cabe citar la reciente decisión de la Comisión [8] de bloquear la propuesta de fusión[9] de dos empresas norteamericanas: General Electric y Honeywell. Según el artículo 1 de esta decisión, adoptada en julio de 2001, la fusión de las dos sociedades generaría una «concentración incompatible con el mercado común». La Comisión estableció que las dos sociedades presentaban en el territorio de la Unión un volumen de negocios total de más de 250 millones de euros, y decidió por tanto que la operación notificada poseía una «dimensión comunitaria».

La dimensión extraterritorial del Derecho comunitario es también perceptible en el Derecho de Consumo. Según el artículo 12 de la Directiva relativa a la protección de los consumidores en materia de contratos a distancia [10], un consumidor no quedará privado de la protección que otorga la Directiva por la elección del Derecho de un país tercero como Derecho aplicable al contrato, cuando el Derecho del país tercero confiera una protección menor que el Derecho comunitario, cuando el contrato presente un «vínculo estrecho» con el territorio de uno o más Estados miembros[11]. El concepto de «vínculo estrecho» procede del artículo 7 del Convenio de Roma de 1980. Este artículo establece

---

5 TGI París, *ordonnance du référé* de 20 de noviembre de 2000: http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm.

6 AG Munich, sentencia de 28.5.1998 – 8340 Ds 465 Js 173158/95.

7 BGH, sentencia de 12.12.2000, Az: 1 StR 184/00.

8 Decisión de 3.7.2001, asunto nº COMP/M2220 de acuerdo con el apartado 3 del artículo 8 del Reglamento (CEE) n° 4064/89, Concentración de empresas.

9 En el marco del acuerdo en cuestión, Honeywell debía convertirse en filial al 100 % de General Electric.

10 Directiva 97/7/CE.

11 El apartado 2 del artículo 6 de la Directiva 93/13 sobre las cláusulas abusivas en los contratos celebrados con los consumidores y el apartado 2 del artículo 7 de la Directiva 99/44 sobre determinados aspectos de la venta y las garantías de los bienes de consumo son muy similares al apartado 2 del artículo 12. Ambos insisten en la aplicación del Derecho comunitario y utilizan el término «vínculo estrecho».

que al aplicar la ley de un país determinado, podrá darse efecto a las «disposiciones imperativas» de la ley de otro país con el que la situación presente un «vínculo estrecho».

La jurisprudencia nos proporciona un ejemplo suplementario, al aplicar un razonamiento similar respecto a la Directiva relativa a los agentes comerciales independientes [12]. El Tribunal de Justicia europeo resolvió [13] que, cuando un agente comercial que ejerce su actividad en el territorio comunitario trabaje para un empresario establecido fuera de la Comunidad, este empresario no puede soslayar las obligaciones de la Directiva en virtud de una disposición contractual que estipule que el contrato se rige por la ley de un país tercero. El Tribunal de Justicia declaró que el Derecho comunitario debe aplicarse cuando «la situación tenga una relación estrecha con la Comunidad».

El sector del transporte aéreo nos proporciona otro ejemplo, más práctico. El Consejo elaboró un Reglamento titulado «Código de conducta para los sistemas informatizados de reserva (SIR)»[14]. Este Reglamento (que regula la utilización de los sistemas SIR) se aplica «a los sistemas informatizados de reserva [...] cuando sean ofrecidos para su uso y utilizados en el territorio de la Comunidad o en ambos casos, con independencia de la condición o nacionalidad del vendedor del sistema, o [...] la ubicación de la correspondiente unidad central del procesamiento de datos». Por lo tanto, si un sistema es accesible en la UE, aunque el equipo central del sistema no esté ubicado en la UE (y los datos se introduzcan en este sistema mediante terminales situados en la UE o fuera de ella), la legislación comunitaria se aplica automáticamente.

Por lo tanto, tras examinar la aplicabilidad de la legislación comunitaria en estos casos que presentan una dimensión extraterritorial podemos concluir que generalmente se aplican criterios similares. Tanto si el requisito es que la relación presente una «dimensión comunitaria» o «un vínculo estrecho» con la Comunidad, en determinadas situaciones, el Tribunal de Justicia europeo, el Parlamento Europeo y el Consejo, así como la Comisión Europea, consideran adecuado imponer normas comunitarias a entidades no establecidas en el territorio de la UE.

En otros países, por ejemplo en los Estados Unidos de América, los tribunales y las leyes aplican razonamientos similares con el fin de que los sitios web extranjeros estén sujetos a las normas locales: la ley norteamericana *Children's Online Privacy Protection Act* (COPPA) de 1998 se aplica también a los sitios web extranjeros que recogen información personal de niños establecidos en el territorio de los Estados Unidos[15]. Según esta ley federal, el operador de un sitio web dirigido a menores de 13 años (o de un sitio destinado al gran público pero cuyo operador recoja a sabiendas información de niños) debe cumplir las disposiciones de la COPPA. Esta ley regula la información que el operador debe incluir en una política de privacidad, cuándo y cómo un operador ha de obtener un consentimiento parental verificable y cuáles son las responsabilidades del operador en cuanto a protección de la vida privada y la seguridad en línea de los niños. Lo interesante para la cuestión que nos ocupa es que esta ley no se aplica específicamente a las empresas norteamericanas, sino también a las empresas «establecidas en Internet», por lo que, desde el punto de vista de la jurisdicción de la ley, la implantación física del

---

12 Directiva 86/653/CEE.

13 Asunto C-381/98, Ingmar GB Ltd. y Eaton Leonard Technologies.

14 Código de conducta para la utilización de sistemas informatizados de reserva (SIR) (versión combinada de los Reglamentos n° 2299/89, modificado por los Reglamentos nº 3089/93 y 323/99).

15 15 U.S.C. § 6502 (1) (A) (I), al cual hace referencia Joel R.Reidenberg, véase la nota a pie de página n° 5.

sitio web importa poco si el sitio en cuestión opera en los Estados Unidos. Si este es el caso, el sitio web estará sujeto a las leyes norteamericanas aplicables.

Un estudio de Derecho internacional señala que los Estados tienden a utilizar varios criterios alternativos para determinar exhaustivamente el ámbito de aplicación del Derecho nacional, cubrir el mayor número posible de casos y ofrecer la protección más amplia posible a los consumidores y a la industria nacionales. Esta tendencia conduce inevitablemente a aplicar varias leyes nacionales a una situación que implica un elemento transfronterizo. Por lo tanto, los instrumentos jurídicos internacionales intentan determinar los criterios pertinentes de manera neutra y no discriminatoria. No obstante, el intento más reciente de avanzar en un proyecto de convenio relativo a la legislación aplicable a los contratos bajo los auspicios de la «Conferencia de La Haya» fracasó porque los países no pudieron ponerse de acuerdo sobre el criterio decisivo. Este es el quid de la cuestión al abordar la legislación aplicable: encontrar un equilibrio entre los diversos intereses de los países en cuestión.

En este contexto, debe tenerse en cuenta que la Directiva de la UE sobre protección de datos contiene un precepto explícito sobre la legislación aplicable e indica un criterio. Independientemente de que sea o no una disposición fácil de comprender o manejar, el hecho de que esta Directiva aborde esta cuestión esencial representa una gran ventaja para los particulares y las empresas.

2. Artículo 4 de la Directiva 95/46/CE sobre la legislación aplicable

El artículo 4 de la Directiva dice así:
«Derecho nacional aplicable
1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

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

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

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro,

sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. »

Este artículo trata de los casos que plantea la cuestión de la legislación aplicable a operaciones de tratamiento de datos personales: se trata de casos en los que al menos un aspecto del tratamiento de los datos personales sobrepasa las fronteras del Estado miembro. Por ejemplo: una sociedad de márketing directo compila listas de direcciones de consumidores establecidos en varios Estados miembros y las utiliza en un Estado miembro con el fin de proceder al envío de publicidad a estos consumidores. O un sitio web norteamericano coloca un *cookie* en el ordenador de particulares de la UE con el fin de que el sitio web identifique el PC y combine esta información con otras.

La Directiva hace la distinción general entre, por una parte, situaciones donde los elementos transfronterizos se limitan a los Estados miembros de la UE o a territorios situados fuera de las fronteras geográficas de la Unión Europea, pero donde se aplica la legislación de un Estado miembro en virtud del Derecho público internacional (el «caso diplomático»)[16] y, por otra parte, las situaciones donde el tratamiento implica elementos que sobrepasan las fronteras de la Unión Europea[17].

Por lo que se refiere a las situaciones dentro de la Comunidad, el objetivo de la Directiva es doble: evitar lagunas jurídicas (casos en los que no sea aplicable ninguna legislación de protección de datos) y evitar la aplicación doble o múltiple de leyes nacionales. Dado que la Directiva define la legislación aplicable y establece un criterio para determinar la legislación susceptible de solucionar cada caso hipotético, la propia Directiva cumple el papel de la denominada «norma de conflicto» y hace innecesario el recurso a otros criterios de Derecho internacional privado.

Para encontrar una respuesta al problema, la Directiva utiliza como criterio o «factor de relación» el «*lugar de establecimiento del responsable del tratamiento*» o, en otras palabras, el principio del país de origen habitualmente aplicado en el mercado interior. Esto significa en particular lo siguiente:

Cuando el tratamiento se efectúa en el marco de las actividades de un establecimiento del responsable en el territorio de un Estado miembro, serán aplicables las disposiciones nacionales sobre protección de datos de ese Estado miembro.

Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, cada uno de los establecimientos deberá respetar las obligaciones impuestas por las leyes respectivas de los Estados miembros para el tratamiento de los datos efectuado en el marco de sus actividades. No se trata de una excepción al principio del país de origen. Se trata simplemente de su aplicación estricta: cuando el responsable elige tener no uno sino varios establecimientos, no se beneficia de la ventaja que supone que respetar una única legislación sea suficiente para todas las actividades ejercidas en el conjunto del mercado interior. Este responsable debe aplicar en paralelo las leyes

---

16 Este caso no se abordará en el presente documento. Sería necesario destacar también que la Directiva, y en consecuencia el artículo 4, se aplica al tratamiento tanto por el sector privado como por el público de datos personales en el marco del Derecho comunitario. El presente documento de trabajo no aborda no obstante la cuestión de la aplicación del artículo 4 al sector público.

17 Esta distinción se aplica principalmente al responsable del tratamiento. Convendría en cualquier caso aclarar que la aplicabilidad de la Directiva no se ve afectada en modo alguno por el hecho de que un responsable del tratamiento establecido en la UE encargue el tratamiento a alguien establecido fuera de la UE. En ese caso, la Directiva se sigue aplicando al conjunto de las operaciones de tratamiento.

nacionales que corresponden a cada uno de los establecimientos. El Grupo de Trabajo podría tratar este aspecto posteriormente.

La aplicación del principio del país de origen se justifica en un mercado interior donde las leyes nacionales de protección de datos ofrecen una protección equivalente gracias a la armonización de los derechos de las personas en cuanto a protección de datos y las obligaciones de la industria y otros responsables del tratamiento de datos personales. De esta manera, el principio del país de origen, que constituye hasta cierto punto una restricción del ámbito de aplicación de las leyes de los Estados miembros en materia de protección de datos, no repercute negativamente en los derechos o intereses de sus residentes o industria. En efecto, aunque las leyes de los Estados miembros no sean aplicables a todos los tratamientos que impliquen a nacionales o que se desarrollen en el territorio nacional, el hecho de que la legislación de otro Estado miembro sea aplicable tiene un impacto muy limitado, puesto que las dos legislaciones han sido armonizadas por la Directiva y son, en consecuencia, equivalentes. Además, la cooperación entre las autoridades nacionales de protección de datos garantiza la confianza, la seguridad y la aplicación efectiva, cualquiera que sea la legislación aplicable [18].

La situación es diferente en las operaciones de tratamiento cuyos responsables están establecidos en un tercer país. Las legislaciones nacionales de estos terceros países no están armonizadas; la Directiva no es aplicable en estos países y la protección de las personas en cuanto al tratamiento de sus datos personales puede ser limitada o inexistente. El principio del país de origen, vinculado al establecimiento del responsable del tratamiento, ya no es válido para determinar la legislación aplicable. Es necesario cambiar el factor de relación. El Parlamento Europeo y el Consejo decidieron volver a utilizar uno de los factores clásicos del Derecho internacional, a saber: el vínculo físico entre la acción y un sistema jurídico. El legislador europeo eligió el país en el cual se sitúa el equipo utilizado [19]. La Directiva se aplica por tanto cuando el responsable del tratamiento no está establecido en el territorio de la Unión, pero decide tratar los datos con fines específicos y utiliza medios, automatizados o no, situados en el territorio de un Estado miembro.

El objetivo de la letra c) del apartado 1 del artículo 4 de la Directiva 95/46/CE es el siguiente: evitar que una persona no esté protegida en un tratamiento efectuado en su país por la única razón de que el responsable del tratamiento no esté establecido en el territorio comunitario. Puede ocurrir simplemente que el responsable del tratamiento no tenga, en principio, nada que ver con la Comunidad. Pero es también posible que haya responsables del tratamiento que decidan establecerse fuera de la UE para evitar la aplicación de la legislación comunitaria.

Cabe destacar que no es necesario que la persona sea ciudadana europea, que esté físicamente presente o que resida en la UE. La Directiva no hace distinción de nacionalidad o localización porque armoniza leyes de los Estados miembros relativas a derechos fundamentales otorgados a todas las personas, con independencia de su nacionalidad. Así pues, en los casos que se debatirán a continuación, el interesado puede

---

18 Véase la primera frase del apartado 6 del artículo 28 de la Directiva 95/46/CE: «Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo.», y la última frase del mismo apartado sobre su obligación de cooperar.

19 Esto no es así cuando los medios se utilizan solamente para garantizar el tránsito de los datos por el territorio comunitario.

ser un ciudadano norteamericano o chino. Desde el punto de vista de la aplicación de la legislación europea sobre protección de datos, se protegerá a esta persona de la misma manera que a cualquier ciudadano de la UE. Lo que importa es la localización de los medios de tratamiento utilizados.

La decisión del legislador comunitario de someter a la legislación comunitaria de protección de datos el tratamiento que utiliza medios ubicados en la UE refleja por tanto un interés real de proteger a las personas en su propio territorio. A nivel internacional, se reconoce que los Estados pueden ofrecer esta protección. El artículo XIV del AGCS permite prever excepciones a las normas de libre comercio con el fin de proteger a las personas, su derecho a la vida privada y a la protección de los datos, y de aplicar esta ley.

En los apartados siguientes se explican los factores pertinentes para determinar la legislación aplicable:

2.1 Establecimiento

El concepto de establecimiento es pertinente en la letra c) del apartado 1 del artículo 4 de la Directiva en el sentido de que el responsable del tratamiento no está establecido en el territorio comunitario. El lugar de establecimiento del responsable de un tratamiento implica el ejercicio efectivo y real de una actividad a través de acuerdos estables y debe determinarse de conformidad con la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. Según este Tribunal, el concepto de establecimiento implica el ejercicio efectivo de una actividad económica por medio de una instalación permanente en otro Estado miembro por una duración indeterminada[20]. Esta exigencia también se cumple cuando una sociedad se constituye durante un periodo determinado.

Cuando se trata de una sociedad que proporciona servicios mediante un sitio Internet, dicho lugar de establecimiento no se encuentra donde está la tecnología que mantiene el sitio, ni donde se puede acceder al sitio, sino en el lugar donde se desarrolla la actividad económica[21]. Por ejemplo: una sociedad de márketing directo se registra en Londres y desarrolla allí sus campañas para toda Europa. La utilización de servidores en Berlín y París no cambia el hecho de que esté establecida en Londres.

2.2. El responsable del tratamiento

Responsable del tratamiento es un concepto general extraído de la Directiva, que define a la persona física o jurídica que sola o conjuntamente con otros determina los fines y los medios del tratamiento de datos personales (letra d) del artículo 2 de la Directiva 95/46/CE). La definición es neutra por lo que se refiere al lugar de establecimiento del responsable del tratamiento. Es exhaustiva puesto que todo tratamiento de datos debe asignarse a uno o más responsables. En el contexto de la letra c) del apartado 1 del artículo 4 de la Directiva, ello significa que debe haber un responsable del tratamiento en alguna parte con arreglo a la definición de la Directiva. Parece también necesario que el tratamiento tenga lugar en el marco de una actividad sujeta al Derecho comunitario y en consecuencia a la Directiva. El tratamiento realizado por una persona física en el marco de una actividad puramente personal o doméstica no entra en el ámbito de aplicación de la Directiva.

[20] Asunto C-221/89 Factortame [1991], Rec. I-3905, apartado 20.

[21] Directiva 2000/31/CE, considerando n°19.

Para poder aplicar la letra c) del apartado 1 del artículo 4 de la Directiva, el responsable del tratamiento debe *recurrir* a medios para el tratamiento de datos personales (y no solamente para garantizar el tránsito) situados en el territorio de un Estado miembro [22]. Esto parece sugerir que el responsable del tratamiento es activo y que alberga una intención particular. Su decisión en cuanto a las finalidades y los medios del tratamiento incluye este aspecto.

2.3 Medios

La Directiva no incluye una defini ción de este término. El diccionario Collins English define el término inglés *«equipment»* como un conjunto de instrumentos o aparatos reunidos para un fin determinado.

Los PC, los terminales y los servidores, que se pueden utilizar para casi todos los ti pos de operaciones de tratamiento de datos, son ejemplos de «medios».

La Directiva explica que los «medios» pueden ser automatizados o no, siempre que no se utilicen solamente con fines de tránsito de la información por el territorio de la Comunidad.

Un ejemplo típico de medios utilizados exclusivamente para el tránsito son las redes de telecomunicaciones (ejes centrales, cables, etc.), que forman parte de Internet y por las cuales pasan las comunicaciones Internet desde el punto de expedición hasta el punto de destino.

2.4 Recurrir a medios

Para la aplicación de la ley de protección de datos en la UE es esencial determinar cuándo el responsable del tratamiento recurre a medios para el tratamiento de los datos personales (letra c) del apartado 1 del artículo 4 de la Directiva).

El Grupo de Trabajo prefiere adoptar un enfoque prudente al aplicar a casos concretos esta norma de la Directiva sobre protección de datos. Su objetivo es garantizar que las personas se beneficien de la protección de las leye s nacionales de protección de datos y de la supervisión del tratamiento de los datos por las autoridades nacionales competentes si es necesario, tiene algún sentido y el grado de aplicabilidad de la Directiva es razonable, habida cuenta del carácter transfronterizo de la situación.

A tenor de lo anterior, el Grupo de Trabajo considera que no toda interacción entre un usuario de Internet establecido en la UE y un sitio web fuera de la UE conduce necesariamente a la aplicación de la legislación europea sob re protección de datos. El Grupo de Trabajo es de la opinión de que los medios deberían estar a disposición del responsable del tratamiento en el tratamiento de datos personales.

---

[22] Hay que señalar que existe una diferencia entre el término utilizado en la versión inglesa en la letra c) del apartado 1 del artículo 4 «*equipment*» y el término ut ilizado en otras versiones de la letra c) del apartado 1 del artículo 4, más cercanas al término inglés « *means*». La terminología utilizada en estas otras versiones es coherente con la formulación de la letra d) del artículo 2, que define al responsable del tratamiento como la persona que define las finalidades y los medios («*means*» en la versión inglesa) del tratamiento. Sin embargo, es necesario destacar que las anteriores versiones inglesas de la Directiva (por ejemplo, la propuesta de modificación de 199 2) utilizaban también el término « *means*», y que se cambió durante las negociaciones, en una fase muy avanzada por el término « *equipment*», como se puede ver en el texto de la posición común de marzo de 1995.

Además no es necesario que el responsable del tratamiento tenga un control total sobre los medios. El responsable del tratamiento puede tener un control variable de estos medios. El control es suficiente cuando el responsable del tratamiento, al determinar la forma en que estos medios funcionan, toma las decisiones adecuadas en relación con la naturaleza de los datos y su tratamiento. En otras palabras, el responsable determina qué datos se recogen, se almacenan, se transfieren, se modifican, etc., de qué forma y con qué objetivo.

El Grupo de Trabajo considera que el concepto de «recurrir» presupone dos elementos: un determinado tipo de actividad emprendida por el responsable y su intención de tratar datos personales. Esto implica que no todo «recurso» a «medios» dentro de la UE lleva a la aplicación de la Directiva.

No obstante, la facultad de disposición del responsable no debe confundirse con la propiedad o la posesión de los medios, ya sea por el responsable del tratamiento, o por la persona. De hecho, la Directiva no concede ninguna importancia a la propiedad de los medios.

La interpretación presentada por el Grupo de Trabajo concuerda plenamente con la motivación del legislador europeo para la elaboración de la disposición de la letra c) del apartado 1 del artículo 4 de la Directiva. El considerando 20 explica que « *el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva»*. Es el corolario necesario si se quiere lograr el objetivo más ampli o de la Directiva, que es: *«evitar que una persona sea excluida de la protección garantizada por la presente Directiva»*.

3. Ejemplos prácticos

El presente capítulo pretende plasmar la orientación proporcionada por el artículo 4 en soluciones concretas aplicables a casos típicos. Un elemento común en los casos que figuran a continuación es que el usuario de Internet no siempre sabe si el sitio web que va a visitar y al cual va a proporcionar datos (conscientemente o no) está situado en el territorio de la UE o fuera del mismo. Los nombres de dominio que no contienen ningún elemento geográfico no pueden localizarse físicamente sin información complementaria. Incluso cuando incluyen datos geográficos, no puede garantizarse que el sitio web se encuentre efectivamente en un servidor situado en el país indicado.

Caso A : *Cookies*

El responsable del tratamiento decide recoger datos de carácter personal por medio de un fichero de texto (*cookie*) que se coloca en el disco duro del ordenador personal del usuario, mientras que el sitio web o un tercero pueden conservar una copia[23]. En una

[23] Los *cookies* son datos creados por un servidor web que pueden almacenarse en ficheros de texto que pueden colocarse en el disco duro del usuario de Internet, mientras una copia puede conservarse en el sitio web. Son una parte normal del tráfico HTTP, y pueden por tanto

comunicación posterior, el sitio web accede a la información registrada en el *cookie* (y en consecuencia en el PC del usuario) con el fin de que el responsable del tratamiento identifique el PC. Este tiene así la posibilidad de combinar toda la información recogida durante las sesiones anteriores con la información que recogerá durante las sesiones siguientes. De esta forma se pueden crear perfiles de usuario bastante detallados.

Los *cookies* son una parte normal del tráfico HTTP y pueden transportarse sin obstáculos con el tráfico IP. Contienen información sobre la persona que el sitio web que las colocó puede consultar. Un *cookie* puede contener cualquier información que el sitio web desee incluir: páginas visitadas, anuncios consultados, número de identificación del usuario, etc.[24].

La instrucción SET-COOKIE se encuentra en la cabecera de la respuesta HTTP[25], concretamente en hipervínculos invisibles. Si se especifica un periodo d eterminado[26], durante dicho periodo el *cookie* se almacena en el disco duro del usuario de Internet y se vuelve a enviar al sitio web que lo creó (o a otros sitios pertenecientes al mismo subdominio). Este reenvío se efectuará a través de un campo *COOKIE* que formará parte del charloteo del navegador ya descrito y se producirá sin ninguna intervención del usuario.

Tal como se ha explicado anteriormente, el PC del usuario puede considerarse un «medio» con arreglo a la letra c) del apartado 1 del artículo 4 de la Directiva 95/46/CE. Está ubicado en el territorio de un Estado miembro. El responsable decidió utilizarlo para el tratamiento de datos personales y, tal como se explica en los apartados anteriores, tienen lugar varias operaciones técnicas sin un contro l por parte del interesado. El responsable del tratamiento emplea los medios del usuario y no lo hace solamente con fines de tránsito en el territorio de la Comunidad.

El Grupo de Trabajo opina por lo tanto que las condiciones en que pueden recogerse datos personales del usuario mediante la colocación de *cookies* en su disco duro son reguladas por el Derecho nacional del Estado miembro donde se sitúa este ordenador personal.

Como el Grupo de Trabajo destacó en una recomendación anterior[27], debería informa rse al usuario cuando esté previsto que el software de Internet reciba, almacene o envíe un *cookie*. El mensaje debería especificar, en un lenguaje fácilmente comprensible, qué información se pretende almacenar en el *cookie* y con qué objetivo, así como su periodo de validez. Posteriormente, el usuario debería contar siempre con la opción de aceptar o rechazar el envío o almacenamiento de un *cookie* en su totalidad y disponer de opciones

---

transportarse sin obstáculos con el tráfico IP. Un *cookie* puede contener un número único (GUI, identificador global único), que permite una mejor personalización que las direcciones IP dinámicas. Permite al sitio web guardar un rastro de las prácticas y preferencias del usuario.
Los *coo kies* contienen una serie de URL (direcciones) para las cuales son válidos. Cuando el navegador vuelve a encontrar estos URL, envía los *cookies* específicos al servidor web.
Los *cookies* pueden ser de naturaleza diferente: pueden ser permanentes o tener una duración limitada (los denominados *cookies* de sesión).

24 Véase la obra de HAGEL III, J. y SINGER, M: *Net Worth: the emerging role of the informediary in the race for customer information»*, Harvard Business School Press, 1999, p. 275.

25 Técnicamente habla ndo, también es posible implementar *cookies* en *JavaScript* o en los campos <META-HTTP EQUIV> ubicados en el código HTML.

26 Los *cookies* de duración indeterminada se llaman *cookies* de sesión y desaparecen al cerrar el navegador o la conexión.

27 Recomendación 1/99 WP 17 «El tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware».

para determinar los datos que se van a conservar o eliminar de un *cookie*, en función por ejemplo del periodo de validez del *cookie* o los sitios web de envío y recepción[28].

Caso B: JavaScript, pancartas y otras aplicaciones similares

Los JavaScripts son aplicaciones informáticas enviadas por un sitio web al ordenador de un usuario que permiten a servidores remotos ejecutar aplicaciones en el PC del usuario. En función del contenido del programa informático, los JavaScripts permiten mostrar información en una página web, pero también introducir virus en el ordenador (los denominados Java malignos) o recoger y tratar información personal almacenada en el ordenador. Cuando el responsable del tratamiento decide utilizar estas herramientas con el fin de recoger y tratar datos personales, recurre a medios en el sentido de la Direc tiva y deberá cumplir las disposiciones de la legislación comunitaria.

Una empresa de publicidad, gracias a un acuerdo con los propietarios de un sitio (motores de búsqueda, por ejemplo) da la orden a un navegador (y en sentido amplio, al ordenador) del interesado de conectarse no sólo con el motor de búsqueda que desea consultar, sino también con el servidor de la empresa de publicidad. De esta manera, la empresa no sólo tiene la posibilidad de enviar pancartas [29] a la pantalla del interesado, sino también de registrar, por medio del navegador del usuario, datos de la dirección y el contenido que la persona envía al motor de búsqueda. La publicidad en pancartas se coloca en el sitio web solicitado mediante un hipervínculo invisible con la empresa de publicidad[30]. El responsable del tratamiento controla por lo tanto, desde el lugar donde se encuentra, el funcionamiento del navegador para hacer que se conecte y transmita información a un tercero.

Además, para que el cliente reciba la pancarta publicitaria más pertinente, las empresas publicitarias en Internet crean perfiles utilizando *cookies* enviados mediante el hipervínculo invisible. Según la configuración del navegador, el usuario puede darse cuenta de la instalación de un *cookie* y aceptarla o rechazarla. El perfil del cliente está vinculado al número de identificación del *cookie* de la empresa de publicidad, para poder ampliarlo cada vez que el cliente visite un sitio web con el que tiene contrato la empresa de publicidad. Así pues, la recogida suplementari a de datos personales del usuario se realiza mediante su ordenador y sin su intervención, cada vez que el usuario de Internet visita el sitio web que contiene esta pancarta.

La Directiva sería también aplicable a la información recogida por programas esp ía o *spyware*. Estos programas informáticos se instalan secretamente en el PC del usuario, por

---

28 Puede encontrarse más información sobre la naturaleza de los cookies y cómo utilizarlos de forma óptima en «Privacidad en Internet – Un enfoque comunitario integrado de la protección de datos en línea», documento de trabajo, WP 37 5063/00. En la página 17 figura una descripción general: «Los *cookies* son datos que se pueden almacenar en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia».
En la p. 88 se enumeran «anuladores de cookies» y se aborda tanto la respuesta de la industria ante los problemas de protección de la vida privada como los mecanismos de oposición a los cookies utilizados por la industria y los programas independientes *cookie washer*, *cookie cutter* y *cookie master*.

29 Las pancartas son pequeñas ventanas gráficas que aparecen en la parte superior de una página web o están integradas en el contenido del sitio.

30 Para más información, véase el capítulo 8, «Cibermarketing», de WP 37 «Privacidad en Internet».

ejemplo al descargar programas informáticos más importantes (que permiten por ej. escuchar música), con el fin de remitir información personal relativa al interes ado (títulos de su música favorita, por ejemplo). Estos programas informáticos se conocen también con el nombre de aplicaciones E.T., ya que en cuanto se instalan en el ordenador del usuario y se enteran de lo que querían saber, hacen lo que hizo el héroe de Spielberg: llamar por teléfono a casa[31].
Estas nuevas aplicaciones informáticas de seguimiento recurren con frecuencia a JavaScript y otras técnicas similares y utilizan claramente los medios del interesado (ordenador, navegador, disco duro, etc.) para recoger datos y enviarlos a otra parte. Puesto que, por definición, estas tecnologías se utilizan sin informar al usuario (el nombre de «programa espía» no deja lugar a dudas) son una forma de tratamiento invisible e ilegítimo.

*****

El Grupo de Trabajo «Artículo 29» es consciente de que, además de los dos ejemplos mencionados en las anteriores secciones, hay otros casos prácticos relacionados con Internet que pueden plantear dificultades de interpretación, debido en parte a la complejidad técnica de los sistemas utilizados.

El Grupo de Trabajo continuará reflexionando sobre esta cuestión y podría abordar otros casos prácticos a la luz de la experiencia nacional y de los avances técnicos que puedan desempeñar un papel importante en el futuro.

El Grupo de Trabajo quisiera subrayar que, incluso en aquellos casos en que no esté totalmente clara la aplicabilidad de la Directiva, el Grupo se compromete a proseguir el diálogo con las empresas y las organizaciones de terceros países que recopilan datos personales en la Unión Europea, con el fin de fomentar la adopción de normas adecuadas en materia de protección de datos para los interesados.

4. ¿Qué significa en la práctica?

a) Aplicación de los principios que regulan la recogida de datos personales

En todos estos casos, la aplicación de la legislación de la UE sobre protección de datos significa, entre otras cosas, lo siguiente:

- Con el fin de que la recogida de datos personales se realice de forma leal y legal, el responsable del tratamiento deberá definir claramente la finalidad del mismo.

- El responsable del tratamiento deberá también garantizar que los datos sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben.

- La recogida deberá basarse en un motivo legítimo (consentimiento inequívoco, ejecución de un contrato, cumplimiento de una obligación legal, de acuerdo con los

[31] Véase en la portada de la revista Time el artículo de Adam COHEN, de 31 de julio de 2000: *How to protect your privacy: who' s watching you? They' re called E.T. programs. They spy on you and report back by «phoning home». Millions of people are unwittingly downloading them.* (Cómo proteger su vida privada:¿Quién le está observando? Se llaman programas E.T. Le espían y cuentan lo que saben «llamando por teléfono a casa». Mil lones de personas los están descargando sin darse cuenta).

intereses legítimos del responsable del tratamiento, etc.) y el particular tendrá derecho a acceder a sus datos personales, así como a rectificarlos o a suprimirlos.

- Deberá comunicarse a la persona de quien se recaben los datos por lo menos información sobre la identidad del responsable del tratamiento y su representante, los fines de la recogida, los destinatarios y sus derechos [32].

- Otro aspecto importante es la seguridad del tratamiento. Ésta podría obligar al responsable del tratamiento a aplicar desde el principio de la recogida medidas técnicas y organizativas específicas destinadas a proteger los datos contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, revelación o consulta no autorizada, en particular cuando los datos se transmitan a través de una red. Tales medidas garantizarán un nivel de seguridad acorde con los riesgos existentes y con la naturaleza de los datos.

- Por lo que se refiere a la información delicada, existen disposiciones específicas, relativas en particular a los requisitos de seguridad, que regulan su recogida [33].

La recomendación 2/2001 del Grupo de Trabajo proporciona más detalles sobre cómo se aplican las Directivas sobre protección de datos al tratamiento de datos por sitios web, así como sobre algunos requisitos mínimos aplicables a la recogida en línea de datos personales en la Unión Europea [34].

b) Aspectos de procedimiento

De conformidad con lo dispuesto en el apartado 2 del artículo 4 de la Directiva 95/46/CE, el responsable del tratamiento debe también designar a un representante establecido en el territorio del Estado miembro donde se sitúen los medios.

La información relativa a la identidad del responsable del tratamiento y del representante podría incluirse fácilmente en la política de privacidad del sitio web o en la información general de identificación del responsable del sitio web, de forma que el responsable del tratamiento de este sitio web pueda ser identificado y contactado fácilmente.

Convendría recomendar el recurso a un único representante, que actúe en nombre de varios responsables del tratamiento, o prever otras soluciones pragmáticas.

Por lo que se refiere a la notificación de la operación de tratamiento deseada (es decir, la recogida) a las autoridades nacionales de protección de datos, la Directiva prevé varias posibilidades. De acuerdo con la primera frase del apartado 1 del artículo 18, el

---

32 El artículo 10 de la Directiva establece que deberá facilitarse información suplementaria en la medida en que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
En el caso de los *cookies*, la persona debería tener también la posibilidad de aceptar o rechazar su colocación, así como de decidir qué datos desea que se traten y cuáles no.

33 Algunos Estados miembros podrían exigir un control previo antes de autorizar el tratamiento de datos delicados.

34 Véase la recomendación 2/2001, WP 43, sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea. Convendría debatir si todos los elementos mencionados en esta recomendación van a ser también aplicables a la recogida en línea de datos en la UE por responsables del tratamiento establecidos fuera de la UE.

responsable del tratamiento o, en su caso, su representante, deberá efectuar una notificación a la autoridad de control con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos. Según la letra a) del apartado 1 del artículo 19, la notificación incluirá, entre otras cosas, el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante.

Con arreglo al segundo guión del apartado 2 del artículo 18, los Estados miembros podrán disponer la simplificación o la omisión de la notificación en los dos casos siguientes: para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados, o cuando el responsable del tratamiento designe a un encargado de protección de los datos personales, que tenga por cometido hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en materia de protección de datos[35].

El Grupo de Trabajo es consciente de que la aplicación de estas disposiciones podría plantear problemas de orden práctico y estaría dispuesto a dedicar más atención a estas cuestiones posteriormente.

c) Aplicación

Está claro que la aplicación de normas en un contexto internacional no es tan fácil como en un contexto nacional. Los ciudadanos deben ser conscientes (y concienciados) de ello. Sin embargo, existen varias posibilidades que se pueden desarrollar con el fin de alcanzar un nivel razonable de aplicación.

Para alcanzar un buen nivel de aplicación, sería necesario en primer lugar sensibilizar a las organizaciones europeas e internacionales de los requisitos de la Directiva en lo que respecta a la recogida de datos en la Unión Europea. La difusión más amplia posible de esta recomendación sería sólo el primer paso. Se precisarían también soluciones tecnológicas, que proporcionaran una estructura preestablecida para la recogida de datos personales e integraran los requisitos descritos en las herramientas informáticas utilizadas para la recogida de datos personales. El Grupo de Trabajo ya ha mencionado la posibilidad de diseñar procedimientos de autorización de productos, que incluyan un control del respeto de las exigencias legales en cuanto a protección de datos personales. Un sistema europeo de etiquetas/sellos web, abierto también a sitios no europeos, podría ser la base de esta iniciativa.

Además, en determinados casos, un ciudadano de la Unión Europea que tuviera algún problema con un sitio web no europeo podría recurrir a la autoridad nacional de control de la protección de datos. Esta autoridad determinaría si es aplicable la Directiva o la legislación nacional en la materia. En ese caso, esta autoridad podría ponerse en contacto con el sitio web extranjero con el fin de resolver el problema. Si se recurre a un tribunal del Estado miembro donde reside este ciudadano, el tribunal decidirá si es competente sobre el asunto en cuestión (lo que podría ser, según el Derecho procesal internacional, puesto que la parte más afectada es el particular que reside en el mismo territorio que el tribunal). Si el tribunal es competente, procede aplicar el artículo 4 de la Directiva 95/46/CE o la legislación nacional de transposición, y el tribunal puede resolver que el sitio web extranjero ha tratado los datos personales del interesado de manera ilegal y desleal. Muchos terceros países van a permitir el reconocimiento y la aplicación de la

[35] Para las disposiciones específicas de Derecho nacional que aplican este artículo de la Directiva, véase: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

sentencia, pero aunque no lo hagan, algunos ejemplos ponen de manifiesto que el sitio web extranjero puede acatar la sentencia y adaptar su sistema de tratamiento de datos con el fin de establecer buenas prácticas y mantener una buena imagen comercial.

En los terceros países donde existen normas de protección de datos y autoridades de control, la aplicación es obviamente menos problemática.

5. Conclusiones

- El Grupo de Trabajo sobre protección de datos «Artículo 29» considera que una interpretación de las legislaciones nacionales como la que figura en el presente documento de trabajo sería sumamente beneficiosa para conseguir la seguridad jurídica de los sitios web establecidos fuera de la Unión Europea. El Grupo de Trabajo está convencido de que sólo podrá garantizarse un nivel elevado de protección de los particulares si los sitios web establecidos fuera de la Unión pero que utilizan medios situados en el territorio comunitario (véase más arriba) respetan las garantías para el tratamiento de los datos personales, en particular la recogida, y los derechos personales reconocidos a nivel europeo y aplicables de todas formas a todos los sitios web establecidos en la Unión Europea.

- El Grupo de Trabajo sobre protección de datos «Artículo 29» considera que el desarrollo de un programa de promoción de normas europeas pragmáticas de protección de datos ayudaría también a los responsables del tratamiento de terceros países a comprender, aplicar y demostrar mejor el respeto de la privacidad. Un sistema europeo de etiquetas/sellos web, abierto también a sitios web no europeos, podría ser la base de esta iniciativa.

- El Grupo de Trabajo sobre protección de datos «Artículo 29» invita a la Comisión a tener en cuenta el presente documento en sus futuros trabajos.

Hecho en Bruselas, el 30 de mayo de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

10761/02/ES/Final
WP 57

Dictamen 1/2002
relativo al informe del CEN/ISSS sobre la normalización de la protección de la vida privada en Europa

Adoptado el 30 de mayo de 2002

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, Dirección A: Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos. B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.
Dirección Internet: www.europa.eu.int/comm/privacy

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[1],

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:

El Grupo de Trabajo toma nota del trabajo emprendido por el CEN/ISSS en el ámbito de la normalización de la protección de la vida privada en Europa [2] y, en particular, del informe final recientemente publicado, que examina el papel que la normalización podría desempeñar en la protección de los datos y de la vida privada de conformidad con la Directiva 95/46/CE.

El Grupo de Trabajo ha seguido siempre con gran interés la evolución de la normalización en el ámbito de la protección de datos, como se refleja en su dictamen 1/97 [3]. Tal como se indica en el mismo, tales iniciativas pueden contribuir de manera importante a la protección de los derechos fundamentales y la intimidad a escala internacional.

Otros documentos del Grupo de Trabajo, como el documento de trabajo sobre la privacidad en Internet[4], han destacado también la necesidad de establecer mecanismos eficaces y fiables que permitan controlar y evaluar el cumplimiento del marco jurídico aplicable. El Grupo de Trabajo se felicita, por lo tanto, de que un buen número de las recomendaciones que figuran en el informe del CEN/ISSS puedan desempeñar un papel importante a este respecto.

El informe del CEN/ISSS y la aplicación de algunas de sus recomendaciones podrían además ayudar a las autoridades responsables de la protección de datos a sensibilizar a las empresas y a los ciudadanos, y a fomentar el debate público en este ámbito. Otras recomendaciones podrían contribuir a aportar soluciones prácticas para los responsables del tratamiento y ayudarles así a cumplir las obligaciones que se derivan de la Directiva relativa a la protección de datos.

Por consiguiente, el Grupo de Trabajo acoge favorablemente esta iniciativa y anima al CEN/ISSS a proseguir esta valiosa labor en el futuro.

Hecho en Bruselas el 30 de mayo de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

[1] DO L 281 de 23.11.1995, p. 31.
[2] Iniciativa del CEN/ISSS sobre la normalización de la protección de la vida privada en Europa, informe final, 13 de febrero de 2002.
[3] Dictamen 1/97 sobre las iniciativas canadienses relativas a la normalización en materia de protección de la intimidad
[4] «Privacidad en Internet - Enfoque comunitario integrado de la protección de datos en línea», WP 37, adoptado el 21 de noviembre de 2000.

10750/02/ES/Final
WP 58

Dictamen 2/2002
sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones: ejemplo del IPv6

Adoptado el 30 de mayo de 2002

Este Grupo fue creado con arreglo al artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente sobre la protección de datos y la privacidad. Sus tareas figuran en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

Los trabajos de secretaría corren a cargo de la Dirección A (Funcionamiento e Impacto del Mercado Interior, Coordinación y Protección de Datos) de la Dirección General de Mercado Interior de la Comisión, B-1049 Bruselas, Bélgica, despacho nº C100-6/136.
Sitio web: www.europa.eu.int/comm/privacy

EL GRUPO DE PROTECCION DE LAS PERSONAS EN LO REFERENTE AL TRATAMIENTO DE DATOS PERSONALES

Establecido por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995[1],

Vistos el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de esa Directiva,

Visto su reglamento interno y, en particular, sus artículos 12 y 14,

ha adoptado el presente dictamen:

Comunicación de la Comisión sobre el IPv6

El 21 de febrero de 2002, la Comisión Europea adoptó una Comunicación al Consejo y al Parlamento Europeo centrada en la próxima generación de Internet y en las prioridades de acción en la migración al nuevo protocolo Internet IPv6. La presente comunicación se produce en el contexto del actual desarrollo de los servicios de red y de los equipos terminales de telecomunicaciones que pueden conectarse a la red.

El nuevo protocolo Internet fue elaborado con vistas a facilitar y armonizar las posibilidades de conexión a la red mediante equipos terminales múltiples, como teléfonos móviles, ordenadores personales o asistentes digitales personales, mediante instalaciones inalámbricas o por cable.

Si bien estos avances no pueden sino fomentarse, el Grupo desearía destacar la necesidad de estudiar cuidadosa y pormenorizadamente las implicaciones del nuevo protocolo en términos de protección de los datos personales.

El Grupo se congratula de la posición adoptada por la Comisión en su comunicación, según la cual las cuestiones en materia de privacidad deberán tenerse en cuenta en el desarrollo futuro de Internet. No obstante, el Grupo subraya que aún no se han resuelto las cuestiones en materia de privacidad planteadas por el desarrollo del nuevo protocolo IPv6.

En particular, preocupa especialmente la posibilidad de la integración de un número de identificación único en la dirección IP, como prevé el nuevo protocolo. A este respecto, el Grupo lamenta no haber sido consultado antes de la adopción de la Comunicación y expresa su deseo de participar en los trabajos futuros sobre el IPv6 a escala europea.

Aspectos de la protección de datos relacionados con la utilización de identificadores únicos en los equipos terminales de telecomunicaciones

El Grupo toma nota del hecho de que el grupo de trabajo internacional de protección de los datos en las telecomunicaciones ha presentado recientemente un documento de trabajo sobre la cuestión de la utilización de identificadores únicos en los equipos

[1] DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

terminales de telecomunicaciones, y desearía agradecer a este grupo de trabajo la labor realizada en este ámbito.

El Grupo suscribe las conclusiones del documento de trabajo adoptado en Auckland el 27 de marzo de 2002[2], y desearía apoyar sus recomendaciones recordando, en particular, la aplicación de varios principios mencionados explícitamente en la Directiva 95/46/CE relativa a la protección de datos personales y la libre circulación de estos datos, y la Directiva 97/66/CE relativa a la protección de datos personales en el sector de las telecomunicaciones[3].

El Grupo desea recalcar que las direcciones IP atribuidas a los usuarios de Internet son datos personales[4] y están protegidas por las Directivas 95/46/CE y 97/66/CE.

En referencia a la labor ya efectuada sobre la protección de datos personales en Internet[5], el Grupo desea destacar específicamente los siguientes puntos:

- El identificador único de una interfaz, como el que puede integrarse en el IPv6, constituiría un identificador de aplicación general y su utilización está reglamentada como tal en la legislación de los Estados miembros de la UE.

- El principio de proporcionalidad implica que, para lograr un equilibrio entre los derechos fundamentales de los interesados y los intereses de los distintos participantes en la transmisión de datos de telecomunicaciones (tales como empresas y proveedores de servicios de acceso a las telecomunicaciones), se trate el menor número posible de datos personales.

  Este principio tiene consecuencias, por un lado, en el diseño de los nuevos protocolos y aparatos de comunicaciones y, por otro lado, en el contenido de las políticas nacionales relativas al tratamiento de datos de telecomunicaciones:si bien la tecnología es, *per se*, neutra, las aplicaciones y el diseño de nuevos aparatos de telecomunicaciones deben respetar, por defecto, la privacidad. Además, debe evitarse generalizar medidas que

---

[2] Véase el anexo del presente documento.

[3] Se ha modificado la Directiva 97/66 para tener en cuenta la evolución tecnológica. Las disposiciones de la nueva directiva buscan proteger a los usuarios de los servicios de comunicaciones electrónicas disponibles públicamente, con independencia de las tecnologías empleadas.

[4] Como especifica el considerando 26 de la Directiva 95/46, los datos se considerarán personales en cuanto se pueda establecer un vínculo con la identidad del interesado (en este caso, el usuario de la dirección IP) mediante medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona. En el caso de las direcciones IP, el proveedor de servicios de Internet siempre puede establecer un vínculo entre la identidad del usuario y las direcciones IP, tal como podrían hacer otros, utilizando por ejemplo registros disponibles de direcciones IP asignadas o utilizando otros medios técnicos.

[5]
- § Documento de trabajo: Tratamiento de datos personales en Internet, adoptado por el Grupo el 23 de febrero de 1999, WP 16, 5013/99/EN/final;
- § Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptada por el Grupo el 23 de febrero de 1999, 5093/98/EN/final, WP 17.
- § Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.
- § Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, adoptada el 7 de septiembre de 1999, 5085/99/EN/final, WP 25.
- § Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet, adoptado el 3 de febrero de 2000, 5007/00/EN/final, WP 28.
- § Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, presentado por el Grupo operativo sobre Internet, adoptado el 3 de febrero de 2000, WP 29, 5009/00/EN/final.
- § 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 de noviembre de 2000, WP 36.

fuercen la capacidad de identificar sistemáticamente los datos de las telecomunicaciones.

En esta perspectiva, en el marco de una conexión de telecomunicaciones, los proveedores de red o de acceso deben ofrecer a cualquier usuario la opción de utilizar la red o de acceder a los servicios de forma anónima o mediante un seudónimo.

La Directiva 97/66/CE prevé que cualquier usuario tenga la posibilidad de restringir la identificación de la dirección comunicante y conectada. En las comunicaciones por Internet, el anonimato puede conseguirse mediante soluciones como el cambio periódico de las direcciones IP de una persona[6].

- Considerando los riesgos de manipulación y de uso fraudulento de un identificador único, el Grupo recuerda la necesidad de medidas de protección, dado que, en particular, los proveedores de servicios de telecomunicaciones son responsables de la seguridad de los servicios que prestan. En el marco de la legislación de la Unión Europea, los proveedores de acceso están obligados a informar a los abonados de los riesgos residuales de seguridad.

- Los requisitos en materia de privacidad, a los que deben responder los parámetros predefinidos de los aparatos de comunicaciones y los servicios de telecomunicaciones, se han aplicado a escala europea a través de las obligaciones específicas destinadas principalmente a los fabricantes de equipos de telecomunicaciones y a los operadores y proveedores de servicios de telecomunicaciones[7].

Conclusión

El Grupo sostiene firmemente las iniciativas de investigación que tengan como objetivo la elaboración de soluciones técnicas para proteger la privacidad de los datos de telecomunicaciones.

El Grupo es consciente de que varios grupos de trabajo ya han tomado iniciativas destinadas a encontrar soluciones técnicas para determinados riesgos para la privacidad ya identificados, y considera necesario iniciar un diálogo, en especial, con los representantes de estos grupos y, más concretamente, con el Grupo Operativo de Ingeniería de Internet y el Grupo Operativo IPv6.

El Grupo se reserva la posibilidad de tomar medidas adicionales a la hora de evaluar el nuevo diseño de los protocolos, productos y servicios de comunicación y para proseguir el diálogo con los participantes en el diseño de estas nuevas herramientas de comunicación.

---

[6] Algunos proveedores de acceso ya han adoptado esta solución, cambiando aproximadamente cada dos días la dirección IP de sus clientes ADSL.
La aplicación de algunos equipos terminales ya tiene en cuenta las orientaciones del RFC 3041 del Grupo operativo sobre Internet (IETF), «*privacy extensions for stateless address autoconfiguration in Ipv6*», enero de 2001. Los equipos terminales utilizan dos tipos de direcciones: una dirección se genera en base a una dirección única MAC y se utiliza para introducir comunicaciones (por ejemplo, el terminal siempre es accesible mediante esa dirección permanente), y otra dirección generada (pseudo) aleatoriamente, utilizada por iniciativa del terminal para conexiones de salida .
En consecuencia, cuando el terminal (y el usuario que está detrás) sea responsable de la conexión no podrá identificarse mediante su dirección MAC.

[7] Véanse la Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, y la Directiva 99/5 sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, DO L 91 de 7.4.1999.

Anexo

Documento de trabajo sobre la utilización de identificadores únicos de los equipos terminales de telecomunicaciones: ejemplo del IPv6

31ª reunión del grupo de trabajo internacional de protección de datos en las telecomunicaciones, celebrada los días 26 y 27 de marzo de 2002 en Auckland (Nueva Zelanda).

Debido a las previsibles carencias del protocolo utilizado en la actualidad en la mayoría de las conexiones de Internet (IP versión 4), el Grupo Operativo de Ingeniería de Internet (IETF) ha cambiado el diseño del protocolo. Este nuevo protocolo, el IPv6, utiliza una banda de 128 bits, en vez de los 32 bits de la antigua versión, para la creación de cada dirección individual IP en Internet.

Esta nueva dirección, gracias a sus mayores capacidades, presenta muchas ventajas y permite nuevas facilidades tales como la multidifusión (transmisión más rápida de grandes cantidades de datos para varios destinatarios como, por ejemplo, el vídeo en línea), la comunicación vocal a través de Internet (*voice over IP*), etc.

No obstante, el nuevo protocolo también plantea dificultades, al haberse diseñado de tal forma que cada dirección IP puede constituirse parcialmente con una serie única de números al igual que un identificador único global. La introducción del IPv6 puede acarrear mayores riesgos de elaboración de perfiles de actividades de los usuarios de Internet[8].

La siguientes consideraciones preliminares identifican los riesgos y recuerdan los principios de privacidad a tener en cuenta a la hora de utilizar un identificador único en la creación de las direcciones IP.

I. Riesgos identificados

Las características del IPv6 conducen a la identificación de riesgos específicos para la privacidad, que dependerán de la configuración del nuevo protocolo.

- *La elaboración de perfiles* es una cuestión problemática si un identificador único (el identificador de la interfaz, por ejemplo, basado en una dirección única MAC de la tarjeta ethernet) se integra en la dirección IP de cada aparato de comunicación electrónica del usuario. En tal caso, puede establecerse una correspondencia entre todas las comunicaciones del usuario con mucha más facilidad que mediante los actuales *cookies*.

- **Se observan *cuestiones relativas a la seguridad y la confidencialidad*. Estos riesgos están relacionados con el desarrollo de servicios de red, lo que implica la multiplicación del tipo de terminales conectadas a la red mediante el mismo protocolo de comunicación: teléfonos móviles, ordenadores personales, o agentes**

[8] La elaboración global del perfil de actividades de un usuario podrá incluso realizarse cuando se utilice el mismo equipo terminal en redes diferentes.

electrónicos que controlan los aparatos domésticos (calefacción, luz, alarmas, etc.).

El nuevo protocolo IPv6 permite conexiones estables, manteniendo la misma dirección, incluso cuando un terminal se desconecta de la red. En este caso, la seguridad y la confidencialidad son problemáticas, dado que existe un riesgo de identificación de los datos relativos a la localización de este nudo móvil[9].

II. Principios sobre protección de datos aplicables al IPv6

El Grupo considera necesario llamar la atención de todos los responsables de la elaboración y aplicación del nuevo protocolo en lo relativo a los requisitos jurídicos nacionales e internacionales que rigen la privacidad y la seguridad de las telecomunicaciones.

En la actualidad, se reconoce ampliamente que la dirección IP -y, *a fortiori*, un número de identificación único integrado en la dirección– puede considerarse como un dato personal en lo que se refiere al marco jurídico[10].

En la línea de su labor anterior y de las posiciones comunes ya adoptadas a este respecto[11], el Grupo recuerda los siguientes principios, que deben tenerse en cuenta al aplicar el nuevo protocolo de Internet.

La infraestructura y los aparatos técnicos de telecomunicaciones deben diseñarse de tal forma que no se utilice ningún dato personal o se emplee el menor número técnicamente posible de datos personales para el funcionamiento de redes y servicios. El identificador único de una interfaz, tal como se integra en el IPv6, constituiría un identificador de aplicación general.

§ En contradicción con el principio de minimalización de los datos, este uso de un identificador único constituye un riesgo de elaboración de perfiles de las personas basado en el conjunto de sus actividades relacionadas con una red.

§ La protección del derecho fundamental a la privacidad frente a este riesgo de elaboración de perfiles debe primar a la hora de analizar los distintos aspectos del nuevo protocolo como, por ejemplo, su sistema de gestión.

---

[9] Véase, por ejemplo, A. Escudero Pascual, «*Anonymous and untraceable communications: location privacy in mobile iternetworking*», 16 de mayo de 2001; «*Location privacy in Ipv6 – Tracking the binding updates*», 31 de agosto de 2001; http://www.it.kth.se/~aep/

[10] Véase, por ejemplo, a escala europea, la Comunicación de la Comisión sobre la organización y gestión del sistema de nombres de dominio de Internet de abril de 2000, y los documentos adoptados por el Grupo de protección de datos personales del artículo 29, en particular «Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea», WP 37, 21 de noviembre de 2000.

[11] Posición común sobre los perfiles en línea en Internet, adoptada en la 27ª reunión del Grupo los días 4 y 5 de mayo de 2000.

§ Posición común sobre la privacidad y la información sobre la localización en los servicios de comunicaciones móviles (*Privacy and location information in mobile communications services*), adoptada durante la 29ª reunión del Grupo los días 15 y 16 de febrero de 2001.

§ Diez mandamientos para proteger la privacidad en el mundo de Internet
Posición común sobre la incorporación de principios específicos de las telecomunicaciones en los acuerdos de privacidad multilaterales (*Incorporation of telecommunications-specific principles in multilateral privacy agreements*), adoptada durante la 28ª reunión del Grupo los días 13 y 14 de septiembre de 2000.
http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm

§ Los datos de tráfico y, en particular, los datos sobre la localización, merecen una protección específica dado su carácter sensible [12].
Si la información sobre la localización tiene que generarse en el marco de la utilización de aparatos móviles y de otros objetos conectados mediante el IP, esta información deberá protegerse contra la intercepción ilegal y la utilización abusiva. También debe evitarse que la información sobre la localización (y el cambio de esta información sobre la localización en función del movimiento del usuario del móvil) se trasmita sin codificar al destinatario de la información a través del encabezamiento de la dirección IP utilizada.

Los protocolos, productos y servicios deberán diseñarse de forma que se puedan elegir direcciones permanentes o provisionales. Los parámetros predefinidos deberían permitir un nivel elevado de protección de la privacidad.

Dado que estos protocolos, productos y servicios están en constante evolución, el Grupo tendrá que vigilar estrechamente el desarrollo de los mismos y solicitar una reglamentación específica si fuera necesario.

Hecho en Bruselas el 30 de mayo de 2002

Por el Grupo

El Presidente

Stefano RODOTA

[12] Véase la Posición común sobre la privacidad y la información sobre la localización en los servicios de comunicaciones móviles, adoptada durante la 29ª reunión del Grupo los días 15 y 16 de febrero de 2001.

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

11203/02/ES/Final
WP 60

Documento de trabajo

Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea

Aprobado el 2 de julio de 2002

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, 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

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[1],

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 documento de trabajo:

Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea

El Grupo de Trabajo es consciente de la expansión de los servicios de autenticación en línea y de la importancia de disponer de mecanismos seguros de autenticación para garantizar la integridad de algunas transacciones electrónicas, en particular las que implican pagos en línea. Desea subrayar que el desarrollo de estos servicios debe respetar los principios esenciales de la protección de datos. Puesto que en la actualidad .NET Passport es la iniciativa más importante en este ámbito, el Grupo de Trabajo ha emprendido en primer lugar un estudio inicial de este sistema.

Tras un primer análisis efectuado por su Grupo operativo sobre Internet, el Grupo de Trabajo considera que, aunque Microsoft ha adoptado diversas medidas para la protección de los datos, hay una serie de aspectos del sistema .NET Passport que plantean cuestiones jurídicas y que deben examinarse con mayor profundidad:

- La información facilitada a los interesados en el momento de recoger los datos, procesarlos o transferirlos a terceros, situados posiblemente en un tercer país.

- El valor y la calidad del consentimiento dado por los interesados a estas operaciones.

- Las normas de protección de datos aplicadas a los sitios web afiliados a .NET Passport.

- La necesidad y condiciones de uso de un identificador único.

- La proporcionalidad y la calidad de los datos recogidos y almacenados por .NET Passport y transmitidos posteriormente a los sitios afiliados.

- El ejercicio de los derechos de los interesados.

---

1 Diario Oficial L 281 de 23.11.1995, p. 31, disponible en inglés en la siguiente dirección: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

- Los riesgos para la seguridad que plantean estas operaciones.

Por tanto, el Grupo de Trabajo decide llevar a cabo este análisis más exhaustivo, manteniendo cuando sea necesario contactos con Microsoft y otros servicios y entidades, con el fin de evaluar si se aplican correctamente los principios europeos de protección de datos y, en su caso, identificar los elementos de los sistemas que deben modificarse. El Grupo de Trabajo volverá a abordar esta cuestión en su próxima reunión plenaria.

Debido a los cambios continuos del servicio .NET Passport y a la posible evolución de su arquitectura en el futuro y la de otros servicios similares de autenticación, el Grupo de Trabajo seguirá supervisando la situación en este ámbito.

Hecho en Bruselas, a 2 de julio de 2002

Por el Grupo de trabajo

El Presidente

Stefano RODOTA

11190/02/ES/final
WP 61

Dictamen 3/2002

relativo a las disposiciones sobre protección de datos de la propuesta de Directiva relativa a la armonización de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de crédito a los consumidores

adoptado el 2 de julio de 2002

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, Dirección A: Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos. B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.

Dirección Internet: www.europa.eu.int/comm/privacy

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[1],

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:

El Grupo de Trabajo agradece a la Comisión que recabe la opinión del Grupo en una fase tan temprana del proceso de toma de decisiones. En principio, el Grupo preferiría bien una simple referencia a lo dispuesto en la Directiva 95/46/CE, bien propuestas más elaboradas sobre protección de datos. Por consiguiente, es posible que emita un posterior dictamen sobre esta materia a la vista de las posibles novedades.

En este momento, desearía insistir en la importancia de que se incluyan disposiciones pertinentes relativas a la protección de datos en esta Directiva. Por ello expresa su disposición a cooperar con la Comisión en la evolución futura de esta cuestión.

Hecho en Bruselas, el 2 de julio de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

[1] Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/privacy

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29

11194/02/ES
WP 62

Proyecto de documento de trabajo sobre el funcionamiento del acuerdo de puerto seguro

Adoptado al 2 de julio de 2002

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, Dirección A (Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos). B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.
Dirección Internet: www.europa.eu.int/comm/privacy

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[1],

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 aprobado el siguiente documento de trabajo:

[1] Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

Ante la próxima conclusión del primer período de dos años de aplicación de la Decisión de la Comisión de 26 de julio de 2000 relativa al acuerdo de *puerto seguro*, este Grupo de Trabajo ha considerado necesario empezar a examinar el estado de aplicación de dicho acuerdo[2].

En primer lugar, el Grupo de Trabajo tomó nota del documento de trabajo de los servicios de la Comisión recientemente publicado [3], en el que se facilitaba información sobre si se habían introducido todos los elementos del acuerdo de puerto seguro, así como sobre las experiencias iniciales conocidas en relación con los requisitos de transparencia, el funcionamiento de los mecanismos de resolución de litigios y la protección de derechos.

Posteriormente, el Grupo de Trabajo realizó una visita a Washington, los días 13 y 14 de marzo de 2002, durante la cual una delegación efectuó un primer análisis exhaustivo, en cooperación con diversas autoridades competentes, organizaciones no gubernamentales y organismos de resolución de litigios.

La información recopilada tras este primer conjunto de iniciativas resulta bastante útil para destacar la necesidad de colaboración de todas las autoridades implicadas, con el fin de aplicar plenamente el acuerdo.

El Grupo de Trabajo contribuirá en breve al análisis de esta cuestión en el marco de sus tareas de supervisión de la aplicación de las legislaciones nacionales relativas a los flujos transfronterizos de datos y del nivel de protección en terceros países, así como de asesoramiento sobre las medidas adecuadas que deben adoptarse para proteger los derechos y libertades de las personas físicas [4], sin olvidar las directrices que recogen sus seis dictámenes emitidos antes de la adopción de la Decisión de la Comisión de 26 de julio de 2000[5].

En particular, el Grupo de Trabajo desearía examinar de forma constructiva si pueden superarse las posibles diferencias en las opiniones relativas a la aplicación de algunos requisitos del puerto seguro, y cómo resolver los posibles desajustes entre los principios que establece el acuerdo y su aplicación práctica. Asimismo, prestará especial atención a los requisitos de transparencia que deberán cumplir las entidades tanto en lo que respecta a la autocertificación de su adhesión al acuerdo de puerto seguro como a sus políticas de privacidad.

Por consiguiente, el Grupo de Trabajo considera que es conveniente que se le facilite información actualizada, sobre todo respecto a una serie de cuestiones relativas a la aplicación del acuerdo. Sobre la base de esa información, el Grupo de Trabajo podrá

---

2 Decisión nº 520/2000/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, DO 215 de 28.8.2000, p. 7.

3 Documento de trabajo SEC(2002) 196 de 13.2.2002.

4 Apartado 1 del artículo 30 de la Directiva 95/46/CE.

5 Dictamen 4/2000, dictamen 3/2000, dictamen 7/1999, dictamen 4/1999, dictamen 2/1999, dictamen 1/1999.

instar a las autoridades, entidades y empresas afectadas a que renueven sus esfuerzos para mejorar el cumplimiento de los principios y requisitos previos de un acuerdo que se acerca a la conclusión de su periodo inicial de aplicación, que comenzó el 1 de noviembre de 2000, fecha de entrada en vigor del marco del puerto seguro. Asimismo, resulta conveniente disponer de información habida cuenta de la posibilidad de que este acuerdo específico, que está estrechamente vinculado a la experiencia estadounidense, se aplique a otras operaciones que impliquen el tratamiento de datos personales en Estados Unidos.

A tenor de lo anterior, el Grupo de Trabajo considera necesario analizar rápidamente las medidas que deben adoptarse para mejorar el conocimiento en Europa de las posibles violaciones de los principios pertinentes.

Por otro lado, el Grupo de Trabajo estima oportuno evaluar el conocimiento de los interesados sobre la utilización de sus datos personales para otros fines.

De acuerdo con la petición formulada por el Parlamento Europeo en su resolución de 5 de julio de 2000[6], el Grupo de Trabajo invita a las autoridades, las entidades y las asociaciones afectadas a colaborar con el fin de recabar información actualizada y específica, en particular a través de las autoridades nacionales de protección de datos y la Comisión Europea, sobre los siguientes aspectos:

- medidas para aumentar la transparencia de las entidades signatarias, especialmente si la declaración de adhesión al acuerdo de puerto seguro no va acompañada de políticas de privacidad adecuadas;
- la posibilidad de prever mecanismos suplementarios de verificación respecto al procedimiento de adhesión al acuerdo, el cumplimiento de las políticas de privacidad por parte de las entidades que han suscrito el acuerdo de puerto seguro y la posible pérdida de los beneficios del puerto seguro;
- las iniciativas que deberán adoptarse para que se conozcan mejor los requisitos previos para la adhesión a los principios de puerto seguro, también mediante documentos breves y fácilmente comprensibles y la posible integración del *Safe Harbor Workbook;*
- las medidas que deberán adoptarse para perfeccionar los mecanismos de resolución de litigios, mejorar la uniformidad y publicidad de los criterios pertinentes, aumentar la transparencia de los resultados de los litigios y racionalizar sus mecanismos de publicación;
- las dificultades que pueden derivarse de la existencia de múltiples políticas de privacidad declaradas por el mismo operador;
- los criterios de prioridad y las posibles iniciativas suplementarias emprendidas por los organismos estadounidenses competentes y las medidas destinadas a renovar la cooperación entre el Panel europeo de protección de datos, los organismos responsables de la resolución de litigios y la Comisión Federal de Comercio (FTC).

El Grupo de Trabajo considera que convendría recopilar la información mencionada antes del próximo 31 de octubre y se reserva el derecho de emitir un dictamen sobre esta cuestión tan pronto disponga de información actualizada.

[6] Resolución del Parlamento Europeo sobre el proyecto de decisión de la Comisión relativa a la adecuación de la protección ..., publicada en el DO C 121 de 24.4.2001, p. 152.

Hecho en Bruselas, el 2 de julio de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

11081/02/ES/Final
WP 63

Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina

Adoptado el 3 de octubre de 2002

El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la UE sobre protección de datos y 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 está a cargo de: Dirección A (Funcionamiento e Impacto del Mercado Interior, Coordinación y Protección de Datos), Dirección General de Mercado Interior, Comisión Europea, B-1049 Bruselas, Bélgica, Despacho C100-6/136. Internet: www.europa.eu.int/comm/privacy

DICTAMEN DEL 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

sobre el nivel de protección de datos personales en Argentina

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 físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[1], y, en particular, su artículo 29 y la letra b del apartado 1 de su artículo 30,

Visto su Reglamento interno[2], y, en particular, sus artículos 12 y 14,

Considerando lo siguiente:

(1) El Gobierno de la República Argentina solicitó[3] a la Comisión que determinara si Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el artículo 25 de la Directiva.

(2) La Comisión Europea solicitó el dictamen del Grupo de Trabajo al respecto.

HA ADOPTADO EL PRESENTE DICTAMEN:

1. INTRODUCCIÓN: LEGISLACIÓN ARGENTINA SOBRE PROTECCIÓN DE DATOS

La legislación argentina regula la protección de datos personales mediante diversos instrumentos jurídicos, que pueden clasificarse en normas generales y sectoriales.

1.1. Normas generales

Las normas generales resultan de combinar la Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario nº 1558/2001 que, juntos, conforman el régimen jurídico común aplicable a la protección de datos personales.

- ***Constitución argentina***

La Constitución argentina prevé un recurso judicial especial, denominado « *habeas data*», para proteger los datos personales. Se trata de un subtipo del procedimiento

[1] DO L 281, 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

[2] Adoptado por el Grupo de Trabajo en su tercera reunión celebrada el 11.9.1996.

[3] Carta del Embajador de la República Argentina ante la Unión Europea, de 23 de enero de 2002.

contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental. En particular, el tercer párrafo del artículo 43 de la Constitución argentina establece que «toda persona podrá interponer esta acción (es decir, el *habeas data*) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística».

La jurisprudencia argentina ha reconocido el *habeas data* como un derecho fundamental y directamente aplicable.

- ***Ley sobre protección de datos personales, de 4 de octubre de 2000 (Ley 25 326, en adelante denominada «la Ley»)***

La Ley desarrolla y amplía lo dispuesto en la Constitución. Contiene disposiciones sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial *habeas data*.

- ***Decreto Reglamentario nº 1558/2001, de 3 de diciembre de 2001 (en adelante denominado «el Reglamento»)***

Este Reglamento establece las normas de aplicación de la Ley, completa lo dispuesto en ella y clarifica aspectos de la Ley que podrían interpretarse de manera divergente.

Estos tres instrumentos jurídicos constituyen las normas generales de la legislación argentina en materia de protección de datos (en adelante, «la legislación argentina»).

Ámbito de aplicación de la legislación argentina

El Grupo de Trabajo evaluó la adecuación del nivel de protección de datos personales proporcionado en conjunto por la Constitución argentina, la Ley 25 326 y el Decreto Reglamentario nº 1588/2001. Por tanto, el presente dictamen se limita al ámbito de las citadas normas y no es aplicable a situaciones no cubiertas por dichos instrumentos jurídicos. El Grupo de Trabajo ha tenido especialmente en cuenta las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la forma en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento y sobre las situaciones a las que se aplica la legislación argentina de protección de datos.

Ámbito de aplicación material

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales la legislación argentina de protección de datos cubre las situaciones siguientes:

i. *En relación al responsable de la base de datos*

La legislación argentina cubre la protección de:

1) *Los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos públicos*. El Grupo de Trabajo interpreta que el responsable de la base de datos es una institución u organismo público. Dicha interpretación se deduce claramente del artículo 43 de la Constitución y del artículo 1 de la Ley;

2) Los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos privados

   a) *si los archivos, registros o bancos de datos exceden el uso exclusivamente personal*. El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales todo uso que pueda afectar a los derechos del titular de los datos debe considerarse que excede el uso exclusivamente personal;

   o

   b) incluso si los archivos, registros o bancos de datos no exceden el uso exclusivamente personal, si tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

El Grupo de Trabajo interpreta que a) y b) se refieren a situaciones en las que el responsable de la base de datos es una entidad privada, sea persona física o jurídica.

En cuanto a los archivos de datos privados, el Grupo de Trabajo observa que tanto el tercer párrafo del artículo 43 de la Constitución como el artículo 1 de la Ley se refieren a «archivos, registros, bancos de datos u otros medios técnicos privados, destinados a dar informes». La misma redacción aparece en otras disposiciones de la citada Ley, como los artículos 14 (derecho de acceso), 21 (obligación de inscribirse en el Registro), 29 (atribuciones del órgano de control), 33 y 35 (requisitos del recurso judicial *habeas data*) y 46 (disposiciones transitorias). No obstante, la interpretación amplia antes indicada se desprende de varios argumentos expuestos por las autoridades argentinas:

- El artículo 1 del Reglamento proporciona una interpretación jurídica de la Ley. En particular, define jurídicamente el concepto de «archivos, registros, bases o bancos de datos privados destinados a dar informes» como «aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito».

- El artículo 24 de la Ley dispone que «los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21». El artículo 21 de la Ley obliga a inscribir en el Registro las bases de datos privadas *destinadas a proporcionar informes*. El artículo 24 no tendría sentido si la Ley sólo se aplica ra a las bases de datos destinadas a proporcionar informes. Estos dos artículos confirman el paralelismo de las expresiones «bases de datos *destinadas a proporcionar informes*» y «bases de datos *[..] que no sean para un uso*

exclusivamente personal», como establece la definición jurídica del artículo 1 del Reglamento (véase el primer argumento citado anteriormente).

- Por otra parte, cabe mencionar que tanto la Ley como el Reglamento contienen normas sobre tratamiento de datos relativos a la salud (artículo 8 de la Ley) o publicidad directa (artículos 27 de la Ley y el Reglamento), según las cuales dichas bases de datos, aunque exceden el uso exclusivamente personal, no pueden estar destinadas a proporcionar informes. Una vez más, estas normas serían superfluas si la Ley sólo fuera aplicable a las bases de datos destinadas a proporcionar informes.

Según las autoridades argentinas, los tribunales de dicho país han seguido la interpretación amplia mencionada anteriormente [4].

ii. En relación al titular de los datos

En relación con el tratamiento de datos personales, la legislación argentina protege tanto a las personas físicas como a las personas jurídicas. El artículo 2 de la Ley define «titular de los datos» como «toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley», y el artículo 1 de la Ley establece que «las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal». El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales el requisito de disponer de domicilio legal, delegaciones o sucursales en Argentina sólo es aplicable a las personas jurídicas titulares de datos y no a las personas físicas. Por tanto, todas las personas físicas son titulares de datos y están protegidas por la legislación argentina.

iii. En relación al método de tratamiento

La legislación argentina abarca la protección de datos personales tanto si su tratamiento es manual como automático. En particular, el artículo 2 de la Ley define «tratamiento de datos» como «operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias».

iv. En relación a la finalidad de las operaciones de tratamiento

El Grupo de Trabajo observa que la legislación argentina tiene al respecto un ámbito de aplicación general. Ya que ninguna norma define la finalidad de las bases de datos sujetas a la legislación, el Grupo de Trabajo interpreta que ésta se aplica en principio a todos los archivos, registros y bancos de datos sea cual sea su finalidad, salvo si se dispone lo contrario. Sin embargo, el Grupo de Trabajo señala los siguientes aspectos:

– Tratamiento de datos con fines de defensa nacional, seguridad pública o represión de delitos

[4] Cámara Civil de Apelación, Mantovano c/ Banco Regional de Cuyo, 2000; Becker José c/ Banco de la provincia de Buenos Aires, 2002

Estas operaciones están sujetas a la Ley. En dichos supuestos se aplican las normas generales de la Ley y el Reglamento, sin perjuicio de lo dispu esto expresamente en el artículo 23 de la Ley como *lex specialis*, que confirma el principio de limitación de la finalidad.

– Tratamiento de datos con fines periodísticos

El párrafo 3 del artículo 43 de la Constitución dispone que «no podrá afectarse el secreto de las fuentes de información periodística». En la misma línea, el artículo 1 de la Ley afirma que «en ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas».

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales esta norma tiene como objetivo proteger el secreto de las fuentes de información periodística como condición necesaria para salvaguardar el derecho fundamental de libertad de prensa, que constituye u n pilar importante de un Estado democrático. En este sentido, debe protegerse la identidad de la fuente de información periodística, por ejemplo, contra un titular de datos que solicitara acceder a sus datos personales, ya que podrían contener información sobre la fuente de los mismos (según el artículo 14 del Reglamento). Por otra parte, la rectificación de datos incorrectos publicados por los medios de comunicación debe seguir las normas del derecho a obtener rectificación asociado a la libertad de prensa .

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales dicha excepción debe aplicarse de manera restrictiva y no es aplicable a las bases de datos personales sin finalidad periodística aunque su responsable ejerza una actividad periodística (por ejemplo, a la base de datos de recursos humanos de un periódico).

– Tratamiento de datos con finalidad estadística

El artículo 28 de la Ley dispone lo siguiente:

«1. Las normas de la presente ley no se apli carán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida en que los datos recogidos no puedan atribuirse a u na persona determinada o determinable.
2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna».

El Grupo de Trabajo señala que no se trata tanto de una excepción al ámbito general de la legislación como de la aplicación del principio de protección de los datos personales, definidos en el artículo 2 de la Ley como «información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables». Por tanto, el Grupo de Trabajo interpreta que, cuando los titulares de datos son personas físicas o jurídicas determinadas o determinables, la legislación es aplicable plenamente y que ello justifica lo dispu esto en el artículo 28 del Reglamento que afirma que «los archivos, registros, bases o bancos de datos mencionados en el Art. 28

de la Ley n° 25.326 son responsables y pasibles de las multas previstas en el Art. 31 de la ley citada cuando infrinjan sus dis posiciones».

Ámbito territorial

Este aspecto se regula en el artículo 44 de la Ley, según el cual puede establecerse la distinción siguiente:

I. Normas de la Ley aplicables uniformemente en todo el territorio nacional:

- Capítulo I: Disposiciones generales
- Capítulo II: Principios generales relativos a la protección de datos
- Capítulo III: Derechos de los titulares de datos
- Capítulo IV: (Obligaciones de los) usuarios y responsables de archivos, registros y bancos de datos
- Artículo 32: Sanciones penales
- La existencia y características principales del recurso judicial *habeas data* (tal como se establece en la Constitución)

II. Normas de la Ley no aplicables uniformemente en todo el territorio nacional:

- Capítulo V: Órgano de control
- Capítulo VI: Sanciones (que puede imponer el órgano de control)
- Capítulo VII: Acción de protección de los datos personales (*habeas data*): Procedimiento aplicable

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales en este ámbito son aplicables las normas siguientes:

– En cuanto a los archivos, registros y bases de datos interconectados en red a nivel interjurisdiccional (es decir, interprovincial), nacional o internacional: Se considera que estos casos competen a la jurisdicción fed eral y, por tanto, están sujetos a lo dispuesto en la Ley.
– En cuanto a otros tipos archivos, registros y bases de datos: Debe considerarse que dichos casos competen a la jurisdicción provincial y las provincias pueden legislar al respecto. Hasta la fecha, algunas provincias han legislado sobre el procedimiento del recurso *habeas data*.

1.2. Normas sectoriales

Se incluyen normas sobre protección de datos en diferentes instrumentos jurídicos que regulan diversos sectores, como por ejemplo las transacciones con tarj eta de crédito, las estadísticas, la banca o la salud.

2. EVALUACIÓN DEL CARÁCTER APROPIADO DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA LEGISLACIÓN ARGENTINA

El Grupo de Trabajo puntualiza que la presente evaluación del carácter apropiado de la legislación argentina sobre protección de datos se centra en las **normas generales** relativas a dicho ámbito mencionadas en el apartado precedente.

Se han comparado dichas normas con las disposiciones principales de la Directiva, teniendo en cuenta el dictamen del Grupo de Trabajo sobre «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE»[5], que enumera diversos principios que constituyen « un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección» . El resultado del análisis es el siguiente:

2.1. Principios de contenido

Principios básicos

- **Principio de limitación de objetivos -** los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por alguna de las razones contempladas en el artículo 13 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 3 del artículo 4 de la Ley establece que «los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención».

- **Principio de proporcionalidad y de calidad de los datos -** los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, los apartados 4 y 5 del artículo 4 de la Ley establece que «los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el art. 16 de la presente ley». Asimismo, el apartado 1 del artículo 4 de la Ley dispone que «los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieren obtenido».

- **Principio de transparencia -** debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder al apartado 2 del artículo 11 y al artículo 13 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 6 de la Ley establece lo siguiente:

---

[5] WP 12 – Aprobado por el Grupo de Trabajo el 24 de julio de 1998, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

«Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo de que se trate, y la identidad y domicilio de su responsable.
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente.
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos».

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales debe distinguirse entre la fuente de legitimidad del tratamiento y la obligación de informar al titular de los datos.

Por una parte, el tratamiento puede estar basado en diversos motivos lícitos, que están especificados en el artículo 5. Estos motivos incluyen, entre otros, el consentimiento del titular de los datos, la existencia de una fuente de acceso público, el ejercicio de tareas de interés público, una obligación legal o una relación contractual. Del artículo 5 del Reglamento se desprende que si el tratamiento se realiza con el consentimiento del titular, dicho consentimiento debe ser informado, lo que implica que previamente debe haberse facilitado al titular toda la información mencionada en el artículo 6.

Por otra parte, el artículo 6 de la Ley establece que «cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara (sigue una relación de cuestiones relativas al tratamiento)». Aunque la redacción de dicho artículo podría hacer pensar que la obligación de informar al titular de los datos se refiere a los casos en los que el titular facilita los datos por sí mismo y con su consentimiento, las autoridades argentinas señalan que dicha obligación es absoluta, incondicional y no depende del motivo que legitima el tratamiento. La obligación de informar es aplicable siempre, independientemente de si los datos personales se solicitan al titular o a un tercero y de si el tratamiento se realiza en virtud del consentimiento del titular o de cualquier otro motivo lícito incluido en el artículo 5 de la Ley. Por tanto, aunque el tratamiento se realice sin el consentimiento del titular, sigue siendo aplicable la obligación de informarle con arreglo al artículo 6 de la Ley.

- **Principio de seguridad -** el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principi o. En particular, el artículo 9 de la Ley establece lo siguiente:

« 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o

tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad».

- **Derechos de acceso, rectificación y oposición** - el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

En lo relativo al derecho de acceso, el Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 1 del artículo 14 de la Ley establece que «el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos o privados, destinados a proveer informes». Este principio se desarrolla en los restantes apartados del artículo 14 y en el artículo 15 de la Ley, así como en los artículos 14 y 15 del Reglamento.

En cuanto al derecho de rectificación y oposición, el Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 1 del artículo 16 de la Ley establece que «toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos». Este principio se desarrolla en los restantes apartados del artículo 16 de la Ley y en el artículo 16 del Reglamento.

Las excepciones a estos derechos, descritas en el artículo 17 de la Ley, permiten restricciones sólo para los bancos de datos públicos y por un número limitado de motivos importantes como la defensa nacional, el orden y la seguridad públicos, la protección de los derechos e intereses de terceros y cuando dicha información pudiera obstaculizar actuaciones judiciales o administrativas en curso vinculadas con el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. El Grupo de Trabajo considera que dichas excepciones se ajustan a lo dispuesto en el artículo 13 de la Directiva.

- **Restricciones respecto a transferencias sucesivas a otros terceros países** - únicamente deben permitirse transferencias sucesivas de datos personales del país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el apartado 1 del artículo 26 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta en gran medida a este principio. En particular, el apartado 1 del artículo 12 establece que «es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuado».

El apartado 2 del artículo 12 de la Ley incluye excepciones a dicho principio en los casos siguientes:

«a) Colaboración judicial internacional.
b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inc. e) del artículo anterior.
c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislació n que les resulte aplicable.
d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte.
e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico».

El artículo 12 del Reglamento añade a la lista de excepciones el consentimiento expreso a la transferencia por parte del titular de los datos y la transferencia des de un registro público en las mismas condiciones que la consulta, en la línea establecida por la letra f) del apartado 1 del artículo 26 de la Directiva.

El Grupo de Trabajo considera que estas excepciones son más amplias que las previstas en la Directiva , especialmente que las enunciadas en las letras b), c) y d) del apartado 1 del artículo 12. El Grupo de Trabajo lamenta este hecho, preferiría que se limitaran dichas excepciones e invita al Gobierno argentino a trabajar en este sentido.

Principios adicionales aplicables a tipos específicos de tratamiento son:

- **Datos sensibles -** cuando se trate de categorías de datos «sensibles» (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que e l interesado otorgue su consentimiento explícito para el tratamiento.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 2 de la Ley define «datos sensibles» como «datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual». El artículo 7 de la Ley prevé protecciones adicionales para su tratamiento:

«1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las as ociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas compe tentes, en el marco de las leyes y reglamentaciones respectivas».
Asimismo, el artículo 8 de la Ley establece que «los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los

pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional».

- **Márketing directo -** en el caso de que el objetivo de la transferencia de datos sea el márketing directo, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a est e principio. En particular, el artículo 27 de la Ley establece lo siguiente:

«1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa, y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfi les determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo».

- **Decisión individual automatizada -** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplic ada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio en lo relativo a las operaciones de tratamiento realizadas por el sector público, dado que tales decisiones automatizadas están prohibidas. En particular, el artículo 20 de la Ley establece lo siguiente:
«1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.
2. Los actos que resulten contrarios a la disposición precedente serán insanableme nte nulos».

En cuanto al sector privado, el Grupo de Trabajo observa que la legislación argentina no hace referencia a este aspecto. Sin embargo, el Grupo de Trabajo recuerda que una resolución de conformidad debe tener en cuenta todas las circunstancias que rodean a la transferencia de datos personales, y el nivel de riesgo que la transferencia plantea al titular de los datos es un elemento importante dentro de dichas «circunstancias». La legislación argentina prevé garantías para el titular en la prestac ión de servicios de información crediticia, que es un sector destacado en lo relativo a las decisiones individuales automatizadas. Dichas garantías, descritas en el artículo 26 de la Ley y del Reglamento, limitan las categorías de datos que pueden procesar se, la fuente de los datos y el período de tiempo al que pueden hacer referencia. Por tanto, el Grupo de Trabajo considera que la ausencia de una disposición general sobre decisiones individuales automatizadas para el sector privado no debe representar un obstáculo para una resolución de conformidad.

2.2. Mecanismos del procedimiento/de aplicación

El dictamen de 1998 del Grupo de Trabajo señala que para evaluar el carácter adecuado del sistema jurídico de terceros países, es necesario distinguir los objetivos subyacentes de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

– ofrecer 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.

- **Ofrecer un nivel satisfactorio de cumplimiento de las normas -** Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la administración encargados específicamente de la protección de datos.

El Grupo de Trabajo entiende que la legislación argentina ha establecido diversos elementos encaminados a cumplir dicho objetivo. En particular:

(a) Sanciones efectivas y disuasorias

La legislación argentina establece sanciones de diversos tipos y grados, en función de la gravedad de la infracción cometida por los responsables o usuarios de las bases de datos. Pueden identificarse dos categorías de sanciones:

i. *Sanciones administrativas*

Estas sanciones están reguladas en el artículo 31 de la Ley y el Reglamento y pueden consistir en apercibimiento, suspensión, multa de mil pesos ($ 1 000) a cien mil pesos ($ 100 000), clausura o cancelación del archivo, registro o banco de datos. Dichas sanciones podrán ser impuestas por el organismo de control y deberán graduarse atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

Asimismo, los responsables o usuarios de bancos de datos públicos pueden incurrir en responsabilidades administrativas en virtud de las normas generales de servicio público.

ii. *Sanciones penales*

El Código Penal argentino considera que tratar a sabiendas datos falsos o violar la confidencialidad o seguridad de los datos son infracciones penales. El Código prevé penas de prisión de 3 a 6 años (o de 4 años y medio a 9 años cuando del hecho se derive perjuicio a alguna persona) y la inhabilitación para desempeñar cargos públicos en el caso de los funcionarios.

El Grupo de Trabajo entiende que dichas sanciones son efectivas y disuasorias, y que pueden inducir de forma satisfactoria a desistir de tratar ilegalmente datos personales.

(b) El órgano de control de protección de datos

La legislación argentina prevé la creación de un órgano de control de protección de datos. Con arreglo al artículo 29 de la Ley, el órgano de control deberá realizar todas las acciones necesarias para cumplir los objetivos y demás disposiciones de la Ley. A tal efecto, el órgano de control ejercerá diversas funciones, entre las que se incluyen funciones de asistencia y asesoramiento, la adopción de normas y reglamentaciones en el desarrollo de la Ley, el mantenimiento de un censo de bases de datos y el control de la observancia de la legislación por parte de las bases de datos. El órgano de control goza de diversas atribuciones, como solicitar autorización judicial para acceder a locales o equipos de tratamiento de datos, solicitar información a las entidades públicas y privadas, imponer sanciones administrativas, constituirse en querellante en acciones penales y controlar el cumplimiento de los requisitos y garantías para inscribir bancos de datos privados en el Registro.

En virtud del artículo 29 del Reglamento, se creó la Dirección Nacional de Protección de Datos Personales (DNPDP), en el ámbito del Ministerio de Justicia y Derechos Humanos, como órgano de control. El Director ejercerá sus funciones con plena independencia, sin estar sujeto a instrucciones. Sus decisiones pueden recurrirse ante los tribunales con arreglo a las normas generales de procedimientos administrativos.

Sin embargo, el Grupo de Trabajo resalta que el Director del órgano de control de protección de datos es designado y puede ser destituido por el Ministerio de Justicia y Derechos Humanos, que también decide sobre el personal de dicho organismo, integrado en la estructura del Ministerio de Justicia. El Grupo de Trabajo considera que tal situación no garantiza que el organismo pueda actuar con plena independencia y, por tanto, insta a implementar los elementos necesarios a tal efecto, incluído un cambio en el procedimiento para designar y destituir al Director del organismo.

Con arreglo al artículo 44 de la Ley, el Grupo de Trabajo entiende que la DNPDP puede considerarse «jurisdicción federal» y que, por tanto, será responsable de controlar los registros, archivos o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional. En otros casos, dichos registros, archivos o bancos de datos estarán bajo jurisdicción provincial y, por tanto, fuera de la jurisdicción de la DNPNP. El Grupo de Trabajo invita a crear órganos de control de protección de datos en todas las provincias, ya que es importante para garantizar que en todos los casos exista un sistema de verificación directo por parte de la administración y un mecanismo institucional que permita investigar las denuncias de manera independiente de la vía judicial.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer un buen nivel de cumplimiento de las normas.

- **Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos -** El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

El grupo de Trabajo observa que la legislación argentina ha establecido diversos elementos encaminados a cumplir este objetivo. En particular:

***(a) El recurso judicial* habeas data**

Como se ha mencionado anteriormente, la Constitución argentina prevé un recurso judicial especial para pro teger los datos personales, conocido como «*habeas data*». Se trata de un subtipo del procedimiento contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental. En particular, el tercer párrafo del artículo 43 de la Constitución argentina establece que «toda persona podrá interponer esta acción (es decir, el *habeas data*) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística».

Las normas legislativas que promulgan dicho recurso constitucional están incluídas en los artículos 33 a 43 de la Ley. El *habeas data* está concebido como un recurso judicial simplificado y rápido que los titulares de dato s pueden utilizar contra los responsables o usuarios de bases de datos. El Gobierno argentino ha aclarado que, de acuerdo con lo comentado en relación al ámbito de la protección de datos en la legislación argentina, este recurso puede utilizarse contra los responsables o usuarios de cualquier base de datos pública o privada (y no sólo de bases de datos privadas destinadas a dar informes), si exceden el uso exclusivamente personal. Dicho aspecto ha sido confirmado por sentencias judiciales en este sentido.

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales la Ley amplía el ámbito de lo dispuesto en la Constitución, al permitir utilizar dicho recurso en los casos en que se presuma el tratamiento de datos personales cuyo registro está prohibido por la Ley. Esto significa que cualquier infracción de las normas de protección de datos puede permitir utilizar el *habeas data*.

Asimismo, el Grupo de Trabajo observa que, en caso de alegar una excepción al derecho de acceso, rectificación o supresión, la carga de la prueba recae sobre el responsable o usuario de los datos.
El recurso *habeas data* permite que una sentencia judicial obligue a suprimir, rectificar, actualizar o declarar confidenciales los datos. El Grupo de Trabajo destaca que la sentencia judicial debe comunicarse al órgano de control, y que ello puede permitir que la DNPDP, en el ámbito de sus competencias, haga aplicar las normas de

protección de datos con respecto a otros titulares de datos afectados que pueden no haber tomado parte en el procedimiento inicial de *habeas data*.

(b) Recursos judiciales generales

Además del *habeas data*, las normas generales de la legislación argentina permiten hacer valer ante los tribunales con arreglo a los procedimi entos generales los derechos y obligaciones relativos a la protección de datos. En particular, el titular de los datos puede incoar un proceso judicial ante un tribunal civil para obtener una compensación por los daños sufridos o para hacer cumplir cualqui era de los derechos reconocidos por la Ley o el Reglamento. Asimismo, pueden incoarse acciones penales por delitos relacionados con el tratamiento de datos personales incluídos en el Código Penal.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer apoyo y asistencia a los titulares de datos individuales 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 -** Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

El Grupo de Trabajo señala que ni la Ley ni el Reglamen to incluyen normas específicas sobre el derecho de quienes resulten perjudicados por una operación de tratamiento ilegal a ser compensados por los daños sufridos. El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto según las cuales, en ausencia de normas especiales, son aplicables las normas generales de la legislación argentina en materia de responsabilidad. Según el caso, pueden ser aplicables las normas en materia de responsabilidad contractual (si el tratamiento se realiza en el marco de una relación contractual entre las partes) o en materia de responsabilidad extracontractual en los demás casos. Las normas argentinas se ajustan en ambos casos a la tradición europea en materia de Derecho Civil y al principio que exige la compensación de los daños ocasionados en caso de manipulación ilegal.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas .

2.3. Otros aspectos

El Grupo de Trabajo observa que el artículo 5 de la Ley permite el tratamiento de datos personales sin el consentimiento del titular de los datos si los datos se obtienen de fuentes de acceso público irrestricto. El Grupo de Trabajo considera que es necesario establecer normas que garanticen que los datos incluídos en una fuente de acceso público irrestricto sean de tal naturaleza que no sea probable que su tratamiento sin el consentimiento del titular pueda suponer un riesgo para los derechos fundamentales y las libertades del individuo y, concretamente, para su derecho a la intimidad. Se sobreentiende que, incluso en el caso de que se incluyan datos personales en una fuente de acceso publico irrestricto, es aplicable todo lo dispuesto en la legislación argentina sobre protección de datos.

3. RESULTADO DE LA EVALUACIÓN

El Grupo de Trabajo insiste en que, para llevar a cabo la presente evaluación de la legislación argentina, el Go bierno de dicho país ha facilitado información sobre la manera en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento, y ha garantizado que las normas en materia de protección de datos se aplican conforme a dicha interpretación. Por tanto, el Grupo de Trabajo ha basado su análisis en las citadas informaciones y garantías del Gobierno argentino, y su dictamen está subordinado al hecho de que, en la aplicación efectiva de las normas de protección de datos en Argentina, se confirmen los citados elementos facilitados por el Gobierno de dicho país. En particular, en lo relativo al ámbito de la legislación argentina, el Grupo de Trabajo ha tenido especialmente en cuenta las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la forma en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento y sobre las situaciones a las que se aplica la legislación de protección de datos. La redacción del presente dictamen se ha basado en dichos supuestos y explicaciones, y no en una experiencia sólida en la aplicación práctica de la legislación, ni a nivel federal ni provincial. Esto es cierto también en lo relativo a que las autoridades argentinas tomen efectivamente en consideración, en un plazo razonabl e, las reservas expresadas anteriormente y las invitaciones a mejorar o modificar los textos legales vigentes.

Como conclusión, en virtud de todo lo anterior, el Grupo de Trabajo asume que Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circu lación de estos datos.

Sin embargo, el Grupo de Trabajo invita también a las autoridades argentinas a tomar las medidas necesarias para solucionar los puntos débiles de los actuales instrumentos legales identificados en el presente dictamen y solicita a l a Comisión Europea continuar el diálogo con el Gobierno argentino con el citado objetivo. En particular, el Grupo de Trabajo insta a las autoridades argentinas a garantizar la aplicación efectiva de la legislación a nivel provincial mediante la creación de los necesarios órganos de control independientes en los casos en los que éstos no existan y, mientras tanto, a buscar soluciones temporales apropiadas que sean conformes con el orden constitucional argentino.

Hecho en Bruselas, el 3 de octubre de 2002

Por el Grupo de Trabajo
El Presidente
Stefano RODOTA

11818/02/ES/Final
WP 64

Dictamen 5/2002

sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9 -11 de septiembre de 2002) sobre la retención sistemática obligato ria de datos sobre tráfico de telecomunicaciones

Aprobado el 11 de octubre de 2002

Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un organismo consultivo independiente europeo sobre protección de datos y de la privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

La Secretaría está a cargo de la Dirección A (Funcionamiento e impacto del mercado único - Coordinación - Protección de datos) de la Dirección General de Mercado Interior de la Comisión Europea, B-1049 Bruselas, Bélgica, Despacho nº C100-6/136.
Website: www.europa.eu.int/comm/privacy

EL GRUPO DE TRABAJO SOBRE LA 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[1],

Vistos el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de esa Directiva,

Visto su Reglamento Interno y, en particular, sus artículos 12 y 14,

Teniendo en cuenta la Declaración de los Comisarios Europeos responsables de la protección de datos en la Conferencia Internacional celebrada en Cardiff (9 -11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciiones,

suscribe todos los términos de esta declaración.

Hecho en Bruselas, el 11 de octubre de 2002.

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

[1] Diario Oficial L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones

Los Comisarios Europeos responsables de la protección de datos han observado con inquietud que, en el marco del tercer pilar de la UE, se consideran propuestas que podrían implicar la retención sistemática obligatoria de datos de tráfico referentes a todo tipo de telecomunicaciones (es decir, detalles sobre el tiempo, el lugar y los números utilizados por teléfono, fax, correo electrónico y otros usos de Internet) durante un período de un año o más, para permitir el posible acceso por los organismos de aplicación de la ley y de seguridad.

Los Comisarios Europeos responsables de la protección de datos tienen serias dudas respecto a la legitimidad y legalidad de unas medidas tan amplias. También quieren llamar la atención sobre el coste excesivo que supondrían las medidas para el sector de las telecomunicaciones y para Internet, así como sobre la ausencia de tales medidas en los Estados Unidos.

Los Comisarios Europeos responsables de la protección de datos han puesto de relieve en varias ocasiones que tal retención sería una invasión incorrecta de los derechos fundamentales garantizados a los individuos por el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, elaborado por el Tribunal Europeo de Derechos Humanos (véase el Dictamen 4/2001 del Grupo de Trabajo del artículo 29 establecido en virtud de la Directiva 95/46/CE, y la Declaración de Estocolmo, de abril de 2000.

La protección de datos sobre tráfico de telecomunicaciones ahora también está prevista ahora por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas (Diario Oficial L 201/37), en virtud de la cual el tratamiento de datos de tráfico está permitido, en principio, para facturación y para pagos de interconexión. Tras debates prolongados y explícitos, la retención de datos de tráfico con vistas a la aplicación de ley debería respetar estrictas condiciones de conformidad con el apartado 1 del artículo 15 de la Directiva: es decir, en cada caso sólo por un período limitado y cuando constituya una medida necesaria proporcionada y apropiada en una sociedad democrática.

Por lo tanto, cuando en casos específicos se deban retener datos de tráfico, debe haber una necesidad demostrable, el período de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la ley, de manera que proporcione suficientes salvaguardias frente a un acceso ilegal o cualquier otro abuso. Una retención sistemática de todas las clases de datos de tráfico para un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso.

Los Comisarios Europeos responsables de la protección de datos esperan que se consulte al Grupo de Trabajo del artículo 29 sobre las medidas que pueden surgir de las negociaciones del tercer pilar antes de que se adopten.

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

11118/02/ES/Final
WP 65

Documento de trabajo sobre las listas negras

Adoptado el 3 de octubre de 2002

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, Dirección de Libre Circulación de la Información y Protección de Datos.
B-1049 Bruselas - Bélgica - Despacho: C100-6/136
Teléfono: directo (32-2) 299 27 19. Centralita: 299 1 11. Telefax: (32-2) 296 80 10.
Dirección Internet: http://europa.eu.int/comm/privacy

LISTAS NEGRAS

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[1],

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 Documento de trabajo.

En primer lugar, el Grupo de Trabajo recuerda que el derecho de las personas a la protección de sus datos personales es un derecho fundamental, reflejado en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Asimismo, se encuentra plasmado en la Carta de los Derechos Fundamentales de la Unión Europea y desarrollado en las Directivas 95/46/CE y 97/66/CE sobre la protección de datos personales.

El derecho fundamental a la protección de datos, como derecho independiente y autónomo del derecho a la intimidad o del derecho al secreto de las comunicaciones privadas, constituye en la práctica un punto de arranque y un elemento novedoso en la sociedad actual. La necesidad de proceder a un adecuado equilibrio entre el mismo y otros derechos fundamentales, por un lado, y otros intereses legítimos de carácter público y privado, con repercusiones tanto a nivel general como individual, por otro, unido a los avances tecnológicos del calado e importancia que estamos presenciando y que hacen posible difundir, disponer y tratar cantidades ingentes de información en poco tiempo y a bajo coste, hacen necesaria la toma en consideración de un aspecto tan importante como es el de la situación que se plantea a un importante número de ciudadanos ante situaciones generadas por circunstancias que abocan a interferencias, en su práctica totalidad no deseadas, en el desenvolvimiento de relaciones comerciales, financieras, profesionales o privadas.

Interferencias en la esfera individual de las personas que se generan por la incorporación de las mismas a bases de datos en las que se aparece identificado en relación con una situación o hechos determinados. Nos estamos refiriendo al fenómeno actualmente denominado como «listas negras», cada vez más extendido y cuestión de compleja definición por varias razones, ya que independientemente de la dificultad de determinar de manera uniforme su concepto y naturaleza, deben tenerse en cuenta las diferencias

[1] Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

existentes entre los Estados miembros causadas por la distinta regulación jurídica y las diferentes tradiciones legales y constitucionales existentes en cada uno de ellos [2].

Abordando de una forma genérica un posible concepto básico de lista negra, podría señalarse que consistiría en la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación.

Dado que cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, constituye un tratamiento de datos personales sujeto a la Directiva 95/46/CE y, consecuentemente, sujeto a las respectivas normativas de transposición de la misma en los distintos Estados miembros, estas llamadas listas negras, para poder existir legalmente, deberán someterse a los principios de legitimación que aparecen en dicha Directiva y respetar los derechos que a los ciudadanos les confiere la misma, salvo que puedan acogerse a alguna de las excepciones previstas en ella.

El presente documento ha sido elaborado en base a la información facilitada por las autoridades de control de los Estados miembros de la Unión Europea a través de un proceso de consulta interna entre los miembros del Grupo de Trabajo del Artículo 29 y en la que se identificaron las principales categorías o tipologías de las mismas y sus características más importantes. El resultado de dicha consulta muestra la existencia generalizada y regulada de determinados tipos de «listas negras», a saber, las relativas a ficheros de deudas, a infracciones criminales o las relativas a la detección del fraude que, de algún modo, encuentran apoyatura o base legal en distintas regulaciones nacionales.

Asimismo, existen otros tipos de «listas negras» cuya existencia no es tan universal como la de las anteriores y, en el caso de que exista, su regulación no es en modo alguno uniforme. Entre ellas se pueden mencionar como más significativas las relativas a infracciones administrativas, negligencias cometidas en ámbitos profesionales, ficheros de carácter laboral o ficheros que incorporan información sobre determinadas conductas individuales que son consideradas inadecuadas por determinados sectores sociales.

Ficheros de deudores y servicios de información de solvencia patrimonial y crédito

Estos ficheros son, quizá, las listas negras que más influencia tienen en un número elevado de ciudadanos y cuya existencia se puede constatar en todos los Estados miembros. También es cierto que son los tratamientos de datos personales los que, en general, suscitan un mayor número de reclamaciones a las autoridades de control de protección de datos europeas. El primer aspecto que debemos mencionar respecto de estos ficheros es la existencia de diversos tipos de regulación en la totalidad de los Estados miembros. En algunos casos se contiene en la normativa de transposición de la

[2] Cabe señalar que en algunos Estados miembros la legislación sobre protección de datos se aplica también a las personas jurídicas.

Directiva 95/46/CE, mientras que en otros aparece en normativas sectoriales de carácter comercial o financiero. No se trata, por lo tanto, de valorar o enjuiciar la legitimidad de la existencia de tales ficheros, que como se ha señalado disponen de base jurídica en los respectivos Estados Miembros, sino de analizar su aplicación y puesta en práctica.
Estas actividades suponen la concertación entre distintos empresarios para transmitirse entre sí, generalmente por medio de una entidad centralizadora, informaciones sobre los clientes, las cuales inciden en las condiciones comerciales o de servicio, de forma directa y significativa. La regulación legal de estas listas se basa en la necesidad de las empresas de contar con información que les permita evaluar los riesgos cuando aceptan prestar un servicio o entregar un bien a crédito y cumplen, de esta manera, también una función de estabilidad y saneamiento del tráfico mercantil.

Por otra parte, cabría hacer una clara distinción entre los ficheros que se denominan ficheros de información sobre solvencia patrimonial y crédito y aquellos destinados a facilitar información relativa al incumplimiento de obligaciones dinerarias.

Los primeros están destinados a la evaluación de las posibilidades económicas y financieras de una persona para hacer frente a una futura obligación crediticia. Los segundos almacenan datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias, con el objetivo de conocer la existencia de anteriores obligaciones impagadas por una persona determinada, lo que de existir, lógicamente, lleva consigo una valoración negativa a la hora de otorgar un nuevo crédito.

En el caso de ficheros en los que se recoge el historial positivo de los pagos de una persona (incluso prohibido en algún Estado miembro, dado que el cumplimiento por parte del deudor de su obligación no supone riesgo alguno para la estabilidad del sistema financiero ni, en principio, dicha comunicación es necesaria para llevar a buen fin una relación contractual entre las partes), la inclusión de esos datos en ficheros comunes debería legitimarse bien en la existencia de legislación que así lo prevea (por ejemplo, para posibilitar a las autoridades financieras competentes evaluar el riesgo general asumido por las entidades financieras) o bien en la existencia de un consentimiento libre, inequívoco, específico e informado por parte del afectado.

En cualquier caso, este tipo de ficheros se ha mencionado aquí ya que conviene tener en cuenta que aunque esta tipología de ficheros comunes relativos a historiales positivos no persiguen la finalidad de estigmatizar a un grupo de personas, objetivo de los ficheros de «listas negras», lo cierto es que su generalización conduciría al mismo resultado a través de una discriminación positiva (*quien está en la lista es bueno, quien no está es malo o, al menos, sospechoso*).

En el caso de los ficheros relativos al incumplimiento de obligaciones dinerarias habría que distinguir a su vez dos tipos de ficheros:

En primer término, **el fichero del acreedor**, en el que éste registra las incidencias de pago que se han ido produciendo respecto de un determinado deudor y cuya fuente es el desenvolvimiento de la relación contractual que mantiene con el deudor. En segundo lugar, el denominado **fichero común**, cuyo responsable es una entidad dedicada a la información sobre solvencia y crédito, a la que el acreedor facilita los datos. Estos ficheros son los conocidos como «ficheros de deudores». Generalmente,

se trata de casos en los que varias entidades (en ocasiones integradas en un solo sector, en otras con un espectro más amplio) celebran un convenio con una tercera empresa en virtud del cual se comprometen a comunicar a dicha entidad las incidencias que tengan con los clientes que no satisfagan sus créditos, siendo dichas incidencias incorporadas al fichero común de morosidad que el responsable pondrá a disposición de los intervinientes, que podrán utilizar dichos datos a la hora de valorar las distintas opciones de crédito que se les planteen.

Este tipo de ficheros, de especial relevancia, ya que comparten y centralizan información, así como su acceso a la misma por parte de las entidades o compañías participantes, constituyen auténticas listas negras de personas que en un momento u otro no han hecho frente adecuadamente a los compromisos financieros que previamente habían asumido. La legitimación para la inclusión de información en los mismos deberá basarse bien en la existencia de determinadas cláusulas contractuales que autoricen al acreedor a comunicar los datos de incumplimiento a un fichero común cuando el mismo se produzca, o bien y fundamentalmente, en la existencia de un interés legítimo del responsable del fichero para conocer la posible existencia de impagados por parte de una persona que acude a solicitarle un crédito.

Es la existencia pues de este interés legítimo de preservación y estabilidad del sistema financiero el que legitima la comunicación a terceros de estas informaciones, si bien dicha comunicación, con graves efectos adversos para el interesado, debe realizarse cumpliendo los principios de la Directiva y someterse a determinadas garantías que salvaguarden también los legítimos derechos de los afectados.

Es, pues, este equilibrio de intereses el que exige que la difusión de datos que puedan acarrear efectos adversos para el interesado, se condicione al cumplimiento de una serie de requisitos y de garantías que se recogen en la Directiva y en la normativa de los Estados miembros. En primer lugar, deben ser tenidos en cuenta los principios relativos a la calidad de los datos, contenidos en el artículo 6 de la Directiva, lo cual implica básicamente lo siguiente:

a) Es necesaria la existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada, así como el requerimiento de pago a quien corresponda el cumplimiento de la obligación. La información incorporada en el fichero debe ser exacta y actualizada. En este apartado adquiere gran relevancia el aspecto relativo al mantenimiento o eliminación de la anotación relativa a una deuda determinada una vez que la misma ha sido satisfecha. En este punto, aunque se percibe una unidad de criterio en la necesidad de limitar temporalmente la permanencia de datos negativos en estos ficheros, hay que destacar que no existe un criterio unánime en la determinación de dicho periodo y los distintos Estados miembros han abordado este problema desde distintas perspectivas. En algunos de ellos no es posible el mantenimiento de dicha anotación una vez que el moroso ha pagado la deuda, aunque lo haya hecho de forma tardía, mientras que en otros sí resulta posible mantener la información durante un periodo máximo que también varía entre los distintos países[3]. No obstante estas divergencias, lo que sí es evidente es que el

[3] A veces el periodo de mantenimiento se establece también en los acuerdos contractuales celebrados entre el acreedor y el deudor, aunque no puede prolongarse más allá de este periodo máximo.

principio de actualización de la información obliga a reflejar claramente el hecho de que la deuda ha sido satisfecha aun cuando el apunte relativo al impago se mantenga más allá de dicho pago.

b) Puesto que la información que se incluye en el fichero común no procede del interesado, debe facilitársele la información prevista en el artículo 11 de la Directiva en cuanto sus datos personales se incluyan en el mismo. Para que dicha información sea correcta, deberán adoptarse aquellos medios razonables que garanticen la recepción de la notificación por parte del interesado Dicha notificación garantiza su derecho a defenderse y evita, de esta forma, posibles errores (como, por ejemplo, los relativos a la identificación del afectado o la inclusión de deudas que el afectado no paga porque no está de acuerdo con el importe o el servicio que se le ha prestado).

c) Otro aspecto de capital importancia es la necesidad de garantizar en toda su extensión el derecho de acceso de los ciudadanos a los datos que obran en estos ficheros y los de rectificación y cancelación en aquellos casos en los que existan errores en la información contenida o, simplemente, se incluyeran datos que no debieran figurar en el fichero. La obstaculización o la negación de estos derechos (por ejemplo, remitiendo al ciudadano a un peregrinaje entre distintos responsables u ofreciéndole información incomprensible) constituye una práctica inaceptable que atenta contra la necesaria transparencia en el funcionamiento de estos ficheros. Por tanto, al notificar la inclusión de datos personales a los ciudadanos, debería nombrarse a un único interlocutor capaz de proporcionar toda la información pertinente y ocuparse del ejercicio de los derechos por el interesado.

d) Otro aspecto relevante respecto de este tipo de ficheros es el relativo a las decisiones individuales automatizadas a las que hace referencia el artículo 15 de la Directiva. Dada la generalización en las entidades financieras de programas informáticos que proporcionan valoraciones respecto de la idoneidad o no de una persona determinada para ser el destinatario de un crédito («credit scoring»), la necesidad de recordar las garantías del mencionado artículo 15 es imprescindible. Estas garantías se concretan en el derecho de una persona a no verse sometida a este tipo de decisiones, excepción hecha de aquellas previstas en una ley, salvo que la misma se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado o existan previsiones que le permitan defender su interés legítimo como, por ejemplo, defender su punto de vista.

   Además, hay que recordar también que, en conexión con este tipo de decisiones, el artículo 12 de la Directiva establece el derecho de los ciudadanos a conocer la lógica utilizada en los tratamientos automatizados que llevan a la toma de este tipo de decisiones.

Infracciones criminales

El artículo 8, en sus apartados 5 y 6, de la Directiva 95/46 CE menciona el tratamiento de datos relativos a infracciones o condenas penales [4], estableciendo, con carácter

[4] Artículo 8 Directiva 95/46/CE: *«(...) 5.El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay*

general, que dichos tratamientos sólo podrán realizarse bajo el control de una autoridad pública, salvo que los Estados miembros adopten excepciones que, por un lado, deberán contar con las garantías adecuadas para no afectar a los derechos fundamentales de los ciudadanos y, por otro, deberán comunicarse a la Comisión Europea.

La legitimación del tratamiento en este tipo de ficheros que incorporan datos relativos a infracciones penales se encuentra en la obligación de los Poderes Públicos de preservar el mantenimiento de la seguridad y el orden públicos, lo que sin duda constituye un principio legitimador de dichos tratamientos, siempre que se cumplan las restricciones mencionadas en el párrafo anterior, de acuerdo con lo que establece el artículo 7 e) de la Directiva.

En relación con los tratamientos de datos de carácter personal relativos a la comisión de infracciones penales, la mayoría de los Estados miembros disponen de ficheros que incorporan este tipo de información y que se encuentran controlados por una autoridad pública.

No obstante lo anterior, diversas Autoridades de control han constatado en sus respectivos países la existencia de ficheros de estas características creados y gestionados de forma privada y referidos, fundamentalmente, a ficheros existentes en grandes supermercados o en compañías de alquiler de vehículos. En los casos de recogida y tratamiento de datos personales de «clientes indeseables» en supermercados, hipermercados o grandes superficies comerciales, las Autoridades de control que se han encontrado con tales situaciones han indicado al responsable del fichero la necesidad de poner fin al tratamiento, determinándose la imposibilidad de admitir este tipo de ficheros en manos de compañías privadas.

Este tipo de tratamiento debe en todo caso respetar los principios de calidad de datos contenidos en la Directiva, y, en particular, los relativos a la exactitud y actualización. Asimismo, especial atención debe prestarse al derecho de rectificación y cancelación de oficio o automática de los datos del afectado, transcurrido el tiempo legalmente establecido y arbitrando, para ello, los distintos mecanismos que lo posibiliten, faciliten y agilicen, ya que la permanencia de información referida a una persona en estos ficheros más allá de los periodos legalmente establecidos puede acarrearle consecuencias perjudiciales.

Ello es especialmente relevante en los casos de existencia de sentencias absolutorias, prescripción de la responsabilidad o rehabilitación. La conservación de tales datos carecería de finalidad. En este punto hay que hacer notar que en la mayoría de los

---

previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos

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

Estados miembros estos aspectos están regulados en las respectivas legislaciones penales, existiendo diferentes variaciones en los criterios establecidos en las mismas.

De igual forma, otro punto fundamental que debe ser tomado en consideración es el del acceso a la información, es decir, determinar las personas o instituciones que se encuentran legitimadas para conocer los datos incorporados a dichos ficheros. Asimismo, el afectado siempre deberá disponer del derecho de acceso a la información relativa a su persona e incorporada en el fichero.

Esta posibilidad de acceso puede dar lugar a situaciones un tanto complejas y problemáticas, como por ejemplo, aquellas en las que el sujeto de los datos sea un demandante de empleo, ya que, en aquellos Estados miembros en los que esté permitido, el empresario, como parte del proceso de selección, podría solicitar al trabajador que le exhiba el contenido de un certificado de antecedentes penales expedido por una autoridad pública responsable del fichero. El candidato obtendría dicho certificado en el que, eventualmente, podrían reflejarse datos sobre condenas penales u otras medidas de seguridad. De esta manera, el empresario obtiene el acceso al contenido de unos datos que de forma directa no tiene legalmente reconocido.

El supuesto presentado puede complicarse aún más ante las situaciones que pueden plantearse como consecuencia de una utilización posterior de tal información por parte del empresario, ya que, en principio, la mera consulta de dicha información puesta a su disposición por parte del candidato durante el proceso de selección no estaría en contradicción con lo establecido en el apartado 5 del artículo 8 de la Directiva, pero sí podría estarlo el tratamiento posterior, ya fuera manual o automatizado.

Detección de fraude

Existen determinados sectores económicos y, fundamentalmente, el sector asegurador, en los que la incidencia de los intentos de defraudar a las compañías que en ellos operan pueden tener tal frecuencia e incidencia en su actividad, que puede conducir a las empresas de dichos sectores al establecimiento de cauces de comunicación de información a través de ficheros comunes que les ayuden a combatir las prácticas fraudulentas y, de este modo, a reducir sus costes operativos.

Se trata de ficheros comunes o centralizados que se nutren de la información existente en las compañías[5], en los que las compañías informan acerca de daños procedentes de clientes sospechosos de comisión de fraude o actuaciones contrarias a las disposiciones en vigor en relación con el sector de que se trate[6].

[5] Véase el punto 2 del apartado relativo a ficheros de deudores y servicios de información de solvencia patrimonial y crédito.

[6] En algunos países, las compañías de seguros también centralizan información sobre clientes que se considera presentan riesgos específicos, aplicando criterios como, por ejemplo, el número de indemnizaciones correspondientes a un cliente en un determinado periodo de tiempo, sin tener siempre en cuenta la responsabilidad del cliente en las mismas. Las compañías de seguros se justifican diciendo que el número de indemnizaciones, incluso sin que el cliente sea responsable, podría considerarse un elemento preliminar para la presunción de fraude. Algunas autoridades responsables de la protección de datos han señalado que algunos aspectos de este tipo de tratamiento suponen un incumplimiento de la

Dadas las similitudes existentes entre ambos (ficheros centralizados, comunicación de datos por parte de terceros, difusión de la información entre los participantes en el sistema, etc.) tanto los problemas como las distintas garantías que deberían adoptarse son similares a los de los ficheros de incumplimiento de obligaciones dinerarias o ficheros de deudores que hemos examinado con anterioridad [7].

El marco legal de dichas listas debe encuadrarse en el respeto y cumplimiento de la regulación de protección de datos de carácter personal: ejercicio del derecho de acceso, notificación al interesado acerca de su inclusión en dicho fichero [8], tiempo de conservación de datos unido a la finalidad para la que se recogen y obligación de eliminación en el momento en que dejan de ser necesarios para la finalidad para la que se recabaron.

Otra cuestión importante es la de la importancia de arbitrar mecanismos necesarios para evitar errores de identificación de las personas incluidas (especialmente relevante cuando se trata de afectados con nombres comunes), de inclusión de deudas erróneas (por ejemplo, de aquellas que están siendo discutidas por el interesado), del importe de la información referente a las cantidades adeudadas, de actualización de la misma en el supuesto de pagos posteriores, etc.[9] De producirse un error de este tipo, deberá procederse a su corrección inmediata en el momento en que se constate, lo cual implica el establecimiento de instrumentos de verificación rigurosos.

En la mayoría de los países, la naturaleza de este tipo de ficheros es privada y, en cuanto a la regulación interna en los distintos Estados miembros, debe señalarse que en términos generales se informa al afectado acerca de su inclusión en el fichero, ya que existe la correspondiente normativa al respecto que así lo determina, si bien la información que se otorga al afectado puede no ser siempre completa y el ejercicio del derecho de acceso puede en ocasiones resultar difícil por las complicaciones que pueden planteársele al afectado.

---

legislación en este ámbito, a menos que existan disposiciones legales que especifiquen garantías adecuadas en el marco del Derecho nacional.

[7] Por ello, los principios legitimadores son similares: la existencia de intereses de carácter público – prevención del fraude, la estabilidad del sistema financiero, saneamiento y protección del curso ordinario del tráfico mercantil, etc.- o legítimo del responsable del fichero, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

[8] Una práctica que evitaría la aparición de errores y problemas sería el establecimiento de un plazo de tiempo razonable entre la notificación o información al interesado acerca de dicha inclusión y la inscripción efectiva de la información en el fichero común, consideración que también podría aplicarse a los ficheros de incumplimiento de obligaciones dinerarias.

[9] Este punto es trasladable a las categorías de listas negras analizadas en el presente documento de trabajo, atendiendo a las especiales características diferenciadoras que concurren en cada una de ellas.

Otras tipologías de listas negras

Tras haber realizado un rápido recorrido por las categorías de «listas negras» más uniformemente distribuidas y reguladas en los Estados miembros y de las que, por lo tanto, existe mayor información, es interesante dedicar otro apartado a aquellas que, aun careciendo de la misma implantación y regulación, no son por ello menos importantes por el enorme impacto que pueden tener en la vida de las personas que se ven incluidas en ellas. Entre estas categorías pueden destacarse las relativas a ficheros con datos adversos sobre trabajadores o candidatos a un puesto de trabajo, ficheros relacionados con cuestiones de salud, comportamientos sociales o políticos y negligencias de profesionales en el ejercicio de su actividad.

Dentro de la tipología expuesta, van a tratarse aquellas listas negras que están basadas en la recogida y difusión de datos especialmente protegidos, ya que, en primer lugar, son las que tienen una mayor incidencia sobre los intereses de los afectados y, al mismo tiempo, parecen ser las más frecuentemente tratadas por las autoridades de control.

Su regulación se contiene en la Directiva 95/46/CE, artículos 8 [10], 13 y 15[11]. En la mayoría de los Estados miembros, y de conformidad con la regulación de la Directiva,

[10] Artículo 8 de la Directiva 95/46/CE: «*1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico,* ***las opiniones políticas****, las convicciones religiosas o filosóficas,* ***la pertenencia a sindicatos****, así como el tratamiento de los datos relativos a la* ***salud*** *o a la sexualidad.*
2. Lo dispuesto en el apartado primero no se aplicará cuando: a) El interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o: b) El tratamiento es necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho Laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o c) El tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, [...];
3. El apartado 1 no se aplicará cuando el tratamiento de 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, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto».

[11] Artículo 15 de la Directiva 95/46/CE: Decisiones individuales automatizadas: « *1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, 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.; 2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: a) Se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo, o: b) Esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado*».

existe la prohibición de tratar datos personales de carácter especialmente protegido si no se otorga el consentimiento explícito.

En algunos de ellos existe la posibilidad de procesar este tipo de datos si se encuentra autorizado por ley o si existe interés legítimo, de carácter público o comercial, para ello[12], ya que la Directiva prevé la posibilidad de que los Estados miembros puedan establecer otras excepciones que legitimen el tratamiento de los datos especialmente protegidos, disponiendo a tal efecto de las garantías adecuadas[13]. Asimismo, en algún Estado miembro, está legal y expresamente prohibida la elaboración de listas negras de trabajadores.

De hecho, en algún Estado miembro se ha desestimado en vía judicial la confección de ficheros en los que incorporaban datos relativos a opiniones políticas, afiliación sindical, cuestiones éticas o informaciones relativas a la salud de trabajadores. Los Tribunales han fallado en contra de la posibilidad de disponer de este tipo de ficheros incluso cuando, en los casos mencionados, únicamente estaban destinados a ser creados dentro del ámbito de la empresa.

En el caso de listas negras que incorporen otra categoría de datos especialmente protegidos, como información relativa a datos de salud, debe señalarse que la existencia de este tipo de ficheros en relación con dichas cuestiones se produce fundamentalmente en la esfera de seguros de vida ofrecidos por las compañías dedicadas a dicho sector. En estos casos, salvo que exista una regulación legal que recoja las debidas garantías, solamente se podrá proceder a la confección de dichos ficheros cuando se cuente con el consentimiento libre, específico, explícito e informado del interesado (que tiene derecho a revocarlo), aunque, también en este caso, deberían tenerse en cuenta los preceptos del artículo 6 de la Directiva y, en particular, la proporcionalidad, la creación de estos ficheros en relación al fin de que se trata. Además, también habrá que comprobar que no exista normativa específica en el Estado miembro de que se trate que prohíba este tipo de prácticas, aun cuando se cuente con el consentimiento del interesado.

En este punto han de mencionarse nuevamente las restricciones que sobre las decisiones individuales automatizadas establece el artículo 15 de la Directiva 95/46/CE.

Como ejemplos específicos de actuaciones en relación con este tipo de listas negras, alguna autoridad de control nacional ha rechazado la existencia de un fichero común, centralizado por una federación de compañías aseguradoras, en el que se incorporaban datos de personas a las que se había denegado la contratación de seguros de vida debido a sus problemas de salud. Por ello, la autoridad de control determinó que fuera o bien suprimido o bien legitimado de acuerdo con las previsiones de la Directiva, dado que consideraba que era suficiente que dispusieran de dicha información las respectivas compañías que contratan con los interesados dichos seguros de vida con las que existe

[12] Véase la letra b) del apartado 2 del artículo 8 de la Directiva 95/46/CE.

[13] Apartado 4 del artículo 8 de la Directiva 95/46/CE: «Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la Autoridad de Control».

una relación contractual cuya naturaleza podría justificar el mantenimiento de dicha información.

En relación con listas negras que incluyen datos especialmente protegidos referidos a ciertas actividades que pueden tener trascendencia social o política, solamente son admisibles y, de hecho, existen en algún Estado miembro (registros o ficheros públicos de personas consideradas de conducta peligrosa) cuando existe una norma o amparo legal que los establece que, al mismo tiempo, especifica las garantías y las limitaciones del acceso a dichos datos. Por último, y continuando con la misma tipología anteriormente señalada, a pesar de existir un acuerdo generalizado entre las autoridades de control respecto de la ilegitimidad de estas listas, en algunos Estados miembros se ha planteado la colisión entre el derecho a la privacidad de los que aparecen incluidos en estas listas y el derecho a la libertad de expresión de los que las difunden, habiéndose pronunciado algunos tribunales a favor de este derecho en algunos casos concretos en algún Estado miembro y en contra en otros lugares.

Independientemente de que no es objeto de este documento analizar las decisiones judiciales ni decidir con carácter universal dónde debe encontrarse el equilibrio entre ambos derechos, sí que es necesario recordar de nuevo que, aun cuando existen casos muy concretos y al amparo de tradiciones legales y constitucionales en las que se interpreta con gran amplitud el derecho a la libertad de expresión, ello no es óbice para que deban respetarse los principios de finalidad, proporcionalidad y actualización de los datos presentes en estos ficheros, así como el ejercicio de los derechos de acceso, rectificación y cancelación, ante cuya denegación las autoridades de control de protección de datos están llamadas a pronunciarse.

CONCLUSIONES Y RECOMENDACIONES

El objetivo del presente documento de trabajo es poner de relieve el fenómeno de la tipología de los ficheros conocidos como «listas negras» en la Unión Europea, describiendo la situación existente en función de la información aportada por las Autoridades de control de los Estados miembros de la Unión Europea a través de un proceso de consulta interna entre los miembros del Grupo de Trabajo del artículo 29, tal y como se menciona en la introducción.

Tras el análisis realizado en el presente documento, se extraen dos conclusiones fundamentales: la incidencia, efectos perjudiciales y consecuencias de esta tipología de ficheros comunes en la esfera privada (y social) de los individuos, así como la existencia de claras divergencias en la regulación de la tipología de ficheros analizada y su puesta en práctica en cada uno de los Estados miembros.

De ahí la importancia de destacar, en términos generales, la conveniencia de disponer de criterios uniformes y armonizados [14] en el marco del tratamiento de datos personales conocidos como «ficheros de listas negras» que arbitren fórmulas que garanticen a los afectados el ejercicio de los derechos reconocidos en la normativa que protege el derecho a la intimidad y a la protección de datos personales. Armonización que, a la luz

[14] En el marco de la Directiva 95/46/CE y de las respectivas legislaciones internas.

del presente documento, adquiere especial relevancia en relación con determinadas cuestiones que a continuación se tratan.

Es importante determinar mecanismos que definan de forma clara y transparente la tipología de datos personales susceptibles de ser tratados, la finalidad de su tratamiento y las garantías a disposición de los afectados (es decir, establecimiento de sistemas de verificación e instrumentos de control de la información tratada), así como las circunstancias y supuestos en los que se permite dicha inclusión. Ello debería articularse en el marco de los principios de legitimación del tratamiento contenidos en el artículo 7 de la Directiva 95/46/CE.

Otro punto fundamental es el relativo a la actualización de la información [15]. Sería de gran importancia tratar de definir parámetros generales que permitan uniformizar plazos de conservación o bloqueo de los datos contenidos en los ficheros. La falta de transparencia en relación con este principio de calidad de datos consagrado en la Directiva puede conducir a una absoluta indefensión del afectado, debido a la inexistencia de mecanismos que a posteriori puedan subsanar el daño causado (es decir, en supuestos de comunicación de datos a terceros sin el conocimiento del afectado).

Un esfuerzo para lograr la máxima armonización en esta cuestión contribuiría por ello a eliminar las diferencias de criterio existentes en la actualidad en los Estados miembros, y facilitaría la labor de los operadores económicos en el marco del derecho de la competencia, en línea con lo dispuesto en el considerando 7 de la Directiva 95/46/CE [16].

Otro aspecto crucial es el derecho que asiste al interesado a ser informado acerca del tratamiento de sus datos personales. Cuando se viola este principio capital, se produce una total indefensión del ciudadano, ya que ni siquiera tiene conocimiento del registro de sus datos personales en una lista negra al no ser él la fuente de los mismos, lo que le impide el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición[17].

---

[15] Letra d) del apartado 1 del artículo 6 de la Directiva 95/46/CE: Principios relativos a la calidad de los datos: «1. Los Estados miembros dispondrán que los datos personales sean: [...] exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas necesarias 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». Véase el apartado del presente documento relativo a «Ficheros de deudores y servicios de información de solvencia patrimonial y crédito».

[16] «Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales , reglamentarias y administrativas de los Estados miembros. »

[17] Artículo 11 Directiva 95/46/CE: «Información cuando los datos no han sido recabados del propio interesado: 1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a

Un aspecto tan esencial como una adecuada regulación del procedimiento de notificación al afectado, con inclusión de criterios de información en tiempo y forma, resulta necesario en el ámbito que nos ocupa, así como una clara indicación de las condiciones, en su caso, para que pueda procederse a su comunicación a terceros[18].

Asimismo, puede sugerirse la articulación de mecanismos que incluyan la información que se da al afectado al denegársele un determinado servicio y, en su caso, posibilidades de comprobación y verificación ulteriores por parte del mismo (en el marco de las garantías anteriormente aludidas). De hecho, la Directiva reconoce el derecho del interesado a no verse sometido a una decisión con efectos jurídicos que le afecte de manera significativa y que se base únicamente en un tratamiento automatizado de datos destinados a evaluar aspectos de su personalidad[19].

Puede también valorarse la procedencia de establecer mecanismos que posibiliten la intervención del afectado, así como la posibilidad de que, de forma motivada y ante supuestos litigiosos, pueda solicitar la inclusión en el fichero de la oportuna información que acredite su posición al respecto.

Otro punto fundamental de máxima importancia en supuestos de ficheros centralizados, comunes y compartidos, es el del establecimiento y aplicación de las medidas de seguridad técnicas y de organización adecuadas, así como las condiciones de acceso a los mismos, obligaciones que recaen en el responsable del tratamiento [20].

Por lo tanto, en línea con lo señalado, y dado que existen determinados sectores que implican servicios de gran importancia (por ejemplo, sector financiero o de telecomunicaciones) en los que la existencia de este tipo de ficheros que incluyen listas negras afecta a un importante número de ciudadanos, el Grupo de Protección de las personas en lo que respecta al tratamiento de datos personales desea concienciar a las instituciones comunitarias acerca de la necesidad de avanzar en la línea marcada por las anteriores conclusiones y destacar la necesidad de que en este ámbito existan criterios

---

continuación, salvo si el interesado ya hubiera sido informado de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: las categorías de los datos de que se trate; los destinatarios o las categorías de destinatarios de los datos; la existencia de derechos de acceso y rectificación de los datos que le conciernen, todo ello en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado. 2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas. » Véase el apartado del presente documento relativo a Ficheros de deudores y servicios de información de solvencia patrimonial y crédito. Deben recordarse los casos en los que la información se recaba del propio interesado.

[18] Véase el apartado 1 del artículo 11 de la Directiva 95/46/CE. «Información cuando los datos no han sido recabados del propio interesado».

[19] Artículo 15 de la Directiva 95/46/CE «Decisiones individuales automatizadas».

[20] Artículo 17 de la Directiva 95/46/CE «Seguridad del tratamiento».

comunes, directrices o líneas de actuación, en el marco de y de conformidad con la Directiva 95/46/CE y con las respectivas legislaciones internas de los Estados Miembros.

Hecho en Bruselas, el 3 de octubre de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

11647/02/ES/Final
WP 66

Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos

Aprobado el 24 de octubre de 2002

El Grupo de trabajo se formó con arreglo al artículo 29 de la Directiva 95/46/CE. Se trata de un organismo europeo independiente y consultivo para la protección de datos y del derecho a la intimidad. Sus misiones se especifican en el artículo 30 de la directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE. Su secretaría se encuentra en:

Comisión Europea, DG Mercado Interior, «Funcionamiento y efectos del mercado interior, coordinación y protección de datos»
B-1049 Bruselas - Bélgica - Despacho: C100-6/136.
Teléfono : línea directa (+32 2) 299.27.19, centralita 299.11.11. Fax : 296.80.10.
Dirección en Internet (sitio en alemán, inglés y francés): http://europa.eu.int/comm/privacy

establecido mediante la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre 1995[1],

vistos su artículo 29 y el punto a) del apartado 1 y el apartado 3 de su artículo 30,

visto su Reglamento interno y, en particular, sus artículos 12 y 14,

ha aprobado el siguiente Dictamen:

1. TEMA DEBATIDO

1.1 Antecedentes y finalidad

A raíz de los atentados del 11 de septiembre de 2001[2], los Estados Unidos aprobaron, el 19 de noviembre de 2001, la *Aviation and Transportation Security Act*[3] (Ley sobre seguridad en el transporte y la aviación), que exige que las compañías aéreas que operen en su territorio les faciliten los datos relativos a los pasajeros y la tripulación (*Passenger Manifest Information*)[4]. Estas transferencias se realizarán en un medio electrónico y deben ser completadas antes del despegue del avión, como máximo 15 minutos después de la salida para los pasajeros. A pesar de que el «*Commissioner of Customs*» (Comisario de aduanas) es el receptor de los datos enviados a los Estados Unidos, las autoridades federales de dicho país también dispondrán de estos datos. El propósito de la transmisión de datos no solo atañe a la seguridad de la aviación, sino que constituye un asunto de orden público en los Estados Unidos.

El 14 de mayo de 2002, los Estados Unidos aprobaron otra ley para reforzar la seguridad fronteriza, que exige que las compañías aéreas que entren y salgan de este país transmitan los datos relativos a los pasajeros y la tripulación al *US Immigration and Naturalization Service*[5] (Servicio de Inmigración y Naturalización de los EE.UU.). En lo que respecta a los pasajeros y la tripulación que salgan de los EE.UU., las transferencias se han de realizar en un medio electrónico, y deben completarse 15 minutos antes del despegue del

---

1 El Diario Oficial L 281 de 23.11.1995, p. 31, puede consultarse en (sitio en alemán, inglés y francés): http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 Con anterioridad al 11 de septiembre de 2001, las compañías aéreas ya transmitían determinados datos a los EE.UU. de manera voluntaria.

3 *Aviation and Transportation Security Act* de 19 de noviembre de 2001 (107-71), *Interim Rules of Dep. of The Treasury (Customs) – Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States* (Registro Federal, 31 de diciembre de 2001) y *Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States* (Registro Federal, 25 de junio de 2002).

4 Se han introducido las mismas obligaciones para el transporte marítimo.

5 *Enhanced Border Security and Visa Entry Reform Act* de 2002, véase también la *Immigration and Nationality Act*.

avión, para que sea posible actualizar o corregir la lista de pasajeros en un espacio máximo de 15 minutos después de la salida. El *US Immigration and Naturalization Service* se reserva el derecho de exigir, si lo considera necesario, que el vuelo regrese al aeropuerto de los EE.UU. en el plazo de una hora desde su salida.

Todos los datos deben transmitirse a una base de datos centralizada[6] conjunta del *US Customs* (Servicio de Aduanas de los EE.UU.) y el *Immigration and Naturalization Service*. Una vez hayan sido transmitidos, estos datos se compartirán con otras agencias federales y dejarán de considerarse datos específicamente protegidos[7].

1.2 Categorías de datos transmitidos

APIS (acrónimo en inglés de «sistema de información avanzada sobr e pasajeros») ha experimentado numerosos avances significativos, especialmente la ampliación de su lista de datos. Al principio, los datos requeridos estaban intrínsecamente relacionados con el vuelo tomado, el visado o el permiso de residencia para los Es tados Unidos, así como con información identificativa como la que figura en los pasaportes.

En particular, la reciente ley estadounidense sobre seguridad fronteriza exige que, para los vuelos que entren y salgan de los EE.UU., se transmitan los siguientes datos a la Oficina de Inmigración de este país: nombre, fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los EE.UU., lugar y fecha de expedición (si corresponde), número de registro extranjero (si corresponde), domicilio en los Estados Unidos durante la estancia, así como cualquier otro dato que se considere necesario para identificar a los viajeros, aplicar las normativas sobre inmigración y proteger la seguridad nacional[8].

Además, en la actualidad se exige, previa petición, la transferencia de datos tratados mediante las reservas y los sistemas de control de salidas (DCS), en especial el llamado *Passenger Name Records* (PNR, registro de nombres de los pasajeros)[9]. Los datos en cuestión no se refieren únicamente a los pasajeros que vuelen a los Estados Unidos, y pueden variar según las distintas compañías aéreas. Pueden referirse a datos identificativos[10] (apellidos, nombre, fecha de nacimiento, número de teléfono), número de reserva del PNR, fecha de la reserva, la agencia de viajes cuando corresponda, la información que se muestra en el billete, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de

---

6 El *Interagency Border Inspection System* (IBIS, Sistema de Inspección Fronteriza Interagencial).

7 Cuando corresponda, estos datos pueden hacerse públicos con arreglo a las leyes que rigen el acceso a la información que posee el sector público.

8 Decisión del Fiscal General tras consultar a l Secretario de Estado y al Secretario de Hacienda estadounidenses.

9 Norma provisional (Registro Federal, 25 de junio de 2002), información sobre el registro de pasajeros (*Passenger Name Record Information*) obligatoria para los pasajeros de vuelos de mat rícula extranjera que entren o salgan de los Estados Unidos.

10 Se menciona específicamente que la lista «tan solo pretende ser ilustrativa respecto a aquellos elementos de los datos que pueda requerir el Servicio de Aduanas».

asiento y datos anteriores del PNR. En estos últimos pueden constar no solo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etc.), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asist encia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (*Frequent Fliers number*)[11].

Asimismo, para los países que participan en el programa de derogación de visados (« *Visa Waiver Program*»), la transferencia de datos biométricos debe convertirse en obligatoria antes de octubre de 2004[12].

1.3 Sanciones

Se contempla la aplicación de fuertes sanciones penales, especialmente la pérdida de derechos de aterrizaje y el pago de cuantiosas multas [13], si no se facilita información, o esta es incorrecta o incompleta.

Respecto a este punto, el Grupo se pregunta hasta qué punto estas medidas, aprobadas unilateralmente, son compatibles con los acuerdos y convenios internacionales sobre tráfico y transporte aéreo, así como con el Derecho nacional aplicable respecto a aquellos países en los que las compañías aére as operan permanentemente.

1.4 Ampliación a otros países

Otros países como Canadá, México [14], Australia, Nueva Zelanda, Sudáfrica y el Reino Unido ya han aplicado o planean aplicar sistemas similares para cubrir sus propias necesidades.

2. COMPATIBILIDAD CON LA DIRECTIVA 95/46/CE

2.1 Aplicación de la Directiva

Los datos facilitados por las compañías aéreas se refieren a personas físicas identificadas . Estos datos son tratados por compañías en la UE (recogidos, registrados, modificados, almacenados, nuevament e modificados, solicitados, utilizados, reenviados, etc.). Como tales, están protegidos por las disposiciones de la Directiva 95/46/CE.

---

[11] Sin embargo, no se dispon e de estos datos, que figuran en las «normas provisionales» publicadas por el Servicio de Aduanas. Lo mismo ocurre con los datos mencionados en la ley 107 -71.

[12] Apartado 203 de la *Enhanced Border Security and Visa Entry Reform Act* de 2002.

[13] Alrededor de 5000 $ por error para el Servicio de Aduanas de los EE.UU. (por ejemplo, nombre del pasajero u otros criterios por debajo de la media semanal aceptada) y 1000 $ por cada nombre incorrecto para el Servicio de Inmigración y Naturalización de los EE.UU..

[14] México también se dispone a enviar todos los datos obtenidos a partir de los vuelos realizados de los Estados Unidos a México.

Además, la evolución del sistema APIS plantea problemas concretos que figuran más abajo. La mayoría caen fuera de la competencia de las compañías aéreas, que se encuentran ante el dilema de que, por un lado, están obligadas a cumplir la ley sobre protección de datos adaptando la Directiva 95/46/CE mientras que, por otro lado, el Derecho estadounidense, respaldado por fuertes sanciones, obliga a dichas compañías a reenviar los datos.

2.2 Información sobre los interesados

Los interesados deberían recibir la información necesaria para garantizar que sus datos reciben un tratamiento adecuado. Dicha información debería incluir la finalidad concreta para la que se tratan los datos en los Estados Unidos, así como sus receptores.

No se puede apelar justificadamente al artículo 13 de la Directiva 95/46/CE para restringir esta obligación cuando la transferencia se realice sistemáticamente y cuando las categorías de información solicitadas ya se hayan hecho parcialmente públicas en los Estados Unidos mediante la aprobación de leyes al respecto. En términos concretos, debería facilitarse esta información a la persona en el momento en que se recojan los datos. Dicha información debe cumplir con los objetivos relativos a su tratamiento en los Estados Unidos y mencionar a sus receptores[15].

2.3 Medidas de seguridad

Con arreglo a la Directiva 95/46/CE, las compañías aéreas están obligadas, sin excepción, a aplicar las medidas de seguridad apropiadas para proteger los datos personales. Da la impresión de que los requisitos técnicos que los Estados Unidos imponen a dichas compañías dejan los datos al alcance de terceros no autorizados.

2.4 Observancia del principio de finalidad

Habida cuenta de los avances que ha experimentado el sistema, tal y como se describe en el punto 2 del apartado 1 del presente texto, la transmisión de datos personales, que va más allá del conjunto de datos que los pasajeros proporcionan normalmente en relación con la organización del viaje, no se puede considerar compatible con la finalidad original de la recogida de datos personales por parte de las compañías aéreas o de las agencias de viajes, en particular con el cumplimiento de sus obligaciones contractuales con respecto a los pasajeros. El punto c) del apartado 1 del artículo 6 de la Directiva 95/46/CE prohíbe el tratamiento posterior de los datos recogidos con fines concretos, explícitos y legales, lo que resulta en cierto modo incompatible con estos fines.

En vista de la gran cantidad y variedad de datos afectados, estos no se pueden considerar adecuados, pertinentes ni imprescindibles en cuanto a los fines que se persiguen al recogerlos y/o tratarlos posteriormente, tal y como se estipula en el punto c) del apartado 1 del artículo 6 de la Directiva 95/46/CE.

Resta por tanto la posibilidad de recurrir al artículo 13 de la Directiva 95/46/CE, que autoriza a los Estados miembros a adoptar medidas legales para limitar el ámbito de aplicación de estas dos obligaciones en la medida en que esta limitación es necesaria para proteger los intereses descritos en la misma disposición (la prevención e investigación de

[15] No es pertinente cuando las personas afectadas son sospechosos que se encuentren bajo investigación.

delitos, seguridad pública, etc.). Evidentemente, sería preferibl e que los Estados miembros adoptasen una perspectiva común al respecto.

2.5 Flujos de datos transfronterizos

La Directiva 95/46/CE estipula que la transferencia de datos personales a terceros países puede realizarse tan solo si estos garantizan un nivel ad ecuado de protección. Los avances de APIS suscitan preocupación al respecto, ya que el tratamiento de los datos facilitados por las compañías aéreas que realizan las autoridades federales estadounidenses no cumplen con este requisito [16]. El ámbito de aplicac ión restringido del «Principio de Puerto Seguro» se refiere a que este no se puede aplicar a la protección de transferencias de datos a las autoridades gubernamentales.

Del mismo modo, parece que tampoco se aplican las excepciones establecidas en el artículo 26 de la Directiva 95/46/CE.

– En estos momentos, el requisito del consentimiento inequívoco no constituiría una solución adecuada, dado que seguiría existiendo una gran preocupación en muchos aspectos. En cualquier caso, no parece que se pida el consentimiento del pasajero, de acuerdo con la ley vigente. La Directiva 95/46/CE define «consentimiento» como «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le concier nan». Puede ser complicado obtener dicho consentimiento, debido entre otras cosas a los problemas reales a la hora de transmitir toda la información necesaria a los pasajeros cuando compran un billete, ya que se trata de sistemas de reserva globales que pe rmiten adquirir pasajes para un vuelo de Europa a los Estados Unidos desde prácticamente cualquier país del mundo por medio de mecanismos muy diversos (distintas compañías y agencias de viajes, etc.). La información que se proporciona a los interesados deb e incluir los puntos establecidos en los artículos 10 y 11 de la Directiva, incluyendo, si corresponde, la inadecuación de las medidas de protección en terceros países.

– Debido al ámbito de los datos transmitidos, resulta difícil apelar a la necesidad de transferirlos para poder cumplir el contrato entre el interesado y la persona responsable del tratamiento de sus datos. De hecho, no se puede considerar «necesaria» la realización de una transferencia de una gran cantidad de datos para cumplir un contrato. La imposibilidad física de que las compañías cumplan con sus obligaciones contractuales, que les lleva a perder sus derechos, no constituye una razón suficiente en este caso. Además, resulta imposible aplicar esta excepción de modo que se contemple la transferencia de datos relativos a personas que no viajen a los Estados Unidos.

– Por el mismo motivo, tampoco parece posible contar con la posibilidad de transferir datos cuando esto resulte necesario para proteger importantes intereses públicos. En primer lugar, no se ha demostrado la necesidad de realizar dicha transferencia y, en segundo lugar, no parece aceptable que una decisión unilateral, tomada por un tercer país por motivos que tan solo obedecen a sus propios intereses públicos, lleve a efectuar de manera periódica y sistemática las transferencias de datos protegidos mediante la Directiva.

---

[16] La ley sobre el derecho a la intimidad aplicable a las autoridades federales estadounidenses solo protege los datos de los ciudadanos del mismo país.

– Por último, parece difícil considerar la transferencia como necesaria para proteger los intereses primordiales del interesado.

No obstante, la Directiva 95/46/CE autoriza la transferencia de datos personales mediante la excepción a la condición de que el tercer país posea un nivel adecuado de protección en el caso de que el controlador (receptor) ofrezca suficientes garantías para la protección de los datos.

Por tanto, podría resultar útil entablar un diálogo entre los Estados miembros y las autoridades estadounidenses con vistas a encontrar una solución que garantice una protección adecuada para los datos transmitidos, para lo cual resultaría adecuado adoptar una postura común de la UE.

2.6 Problemas específicos de la comunicación y el acceso a los datos del PNR tratados en sistemas automatizados de reserva o sistemas de control de salida

Los comentarios aquí realizados son de carácter complementario a los expuestos anteriormente.

2.6.1 Conexiones electrónicas directas entre el Servicio de Aduanas de los EE.UU. y los sistemas de reserva y de control de salida

En los casos en que se prevé que el Servicio de Aduanas de los EE.UU. pueda acceder directamente a los sistemas de información en territorio europeo, y solicitar o recoger datos en lugar de ser los receptores de un flujo convencional de datos transfronterizos, la Directiva en su totalidad puede considerarse completa y directamente aplicable. El punto c) del apartado 1 del artículo 4 establece que la Directiva se aplicará cuando el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de un Estado miembro[17]. No obstante, la aplicación de la Directiva en su totalidad plantea numerosas cuestiones.

2.6.2 Datos relativos a personas que no viajen a los Estados Unidos

Los datos relativos a pasajeros que no viajen a los Estados Unidos no son pertinentes y, por tanto, no deben transmitirse excepto en el marco de acuerdos concretos de Justicia e Interior (asistencia mutua).

---

17 El considerando 20 de la Directiva 95/46/CE estipula «que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deb en adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva». En un Dictamen publicado recientemente, que se centra en la interpretación del ámbito de aplicación del punto c) del apartado 1 del artículo 4 de la Directiva (documento de trabajo relativo a la determinación de la aplicación internacional de la ley sobre protección de datos de la UE respecto al tratamiento de datos personales en Internet por parte de sitios de Internet alojados fuera de la UE, de 30 de mayo de 2002), el Grupo de trabajo del artículo 29 señaló que no es necesario que el controlador ejerza pleno control sobre el equipo, si bien debería determinar qué datos se recogen, almacenan, transfieren, modifican, etc., y con qué finalidad.

2.6.3 Información delicada

El PNR puede contener datos que revelen el origen étnico o racial, las convicciones religiosas u otro tipo de información delicada en el sentido descrito en el artículo 8 de la Directiva 95/46/CE, que en principio prohíbe cualquier tipo de tratamiento de esta información a menos que se cuente con autorizaciones concretas (consentimiento explícito para su tratamiento con fines concretos, datos de carácter claramente público, etc.). Al recurrir al consentimiento se crean muchos problemas como los anteriormente descritos, lo que debería merecer una atención incluso mayor, dada la naturaleza sumamente delicada de estos datos[18].

El apartado 4 del artículo 8 de la Directiva autoriza a los Estados miembros o a las autoridades supervisoras a establecer otras excepciones por motivos de interés público importantes, siempre que se dispongan las garantías adecuadas. En el caso de que se cumplan estas condiciones, los Estados miembros podrían autorizar en consecuencia la transferencia de información delicada contenida en el PNR [19].

2.6.4 Tratamiento de datos mediante los sistemas de reserva y de control de salida (DCS)

Además, la cuestión sobre el acceso al PNR a petición de las autoridades estadounidenses plantea, desde el principio, la controversia sobre la legitimidad del tratamiento de datos que se lleva a cabo en los sistemas de reserva y de control de salida [20]. En particular, solo se pueden tratar los datos si son apropiados, pertinentes y necesarios respecto a la finalidad de su tratamiento. Deberían dejar de tratarse los datos personales en los sistemas de reserva, dado que aquellos dejan de utilizarse para el viaje pa ra el que fueron registrados.

2.7 Transferencias de datos biométricos

La transferencia de datos biométricos se rige por las disposiciones de la Directiva 95/46/CE. Debe señalarse que esta Directiva exige que los Estados miembros determinarán las condicione s en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento. Los identificadores biométricos permiten únicamente la identificación de las personas, y podrían ser objeto de aplicación de esta disposición [21].

---

[18] Conforme al punto a) del apartado 2 del artículo 8 de la Directiva, la legislación de un Estado miembro puede disponer que la prohibición de tratar datos mencionada en el apartado 1 del artículo 8 de la Directiva no pueda levantarse mediante el consentimiento del interesado.

[19] Se sigue aplicando el artículo 13 de la Directiva.

[20] Véase la Recomendación 1/98 sobre los sistemas informatizados de reserva de las líneas aéreas, que también menciona el archivo de datos por un tiempo determinado pa ra resolver litigios, así como el tratamiento de datos relativos a personas que viajan con frecuencia una vez obtenido el consentimiento de los interesados. El Grupo de trabajo del artículo 29 recomienda en principio almacenar los datos en línea solamente durante 72 horas y eliminarlos en un periodo no superior a tres años (con acceso limitado a las peticiones para investigación) o incluso más tiempo (tan solo para cumplir con una obligación legal).

[21] El Grupo de trabajo se encuentra actualmente debatiendo la cuestión de los datos biométricos.

Conclusiones

1. El Grupo de trabajo es consciente de que los Estados soberanos poseen un criterio definido respecto a la información que pueden pedir a las personas que desean acceder a su territorio. Sin embargo, las propuestas actuales en lo que respecta al sistema APIS, si bien se han elaborado en el contexto de abominaciones terroristas, podrían llevar a la divulgación desproporcionada y periódica de información por parte de las compañías aéreas que deben atenerse a los requisitos de la Directiva 95/46/CE. Esta información podría utilizarse con fines regulares relacionados con la inmigración y el control aduanero así como, de un modo más general, para la seguridad nacional de los EE.UU., y podría al menos ser compartida por todas las agencias federales de dicho país.

2. A la luz del reciente desarrollo del sistema APIS, el Grupo de trabajo opina que, al cumplir con los requisitos de los EE.UU., se crean problemas respecto a la Directiva 95/46/CE. La mayoría de las cuestiones en juego se encuentran fuera de la competencia de las compañías aéreas, y deberían ser los Estados miembros, y la Comisión si resulta necesario, quienes se ocupasen de ellas.

3. En esencia, el Grupo de trabajo opina que deberían impedirse las transferencias de datos relativos a personas que no viajen a los Estados Unidos, excepto bajo acuerdos específicos de cooperación relacionados con Justicia e Interior.

4. Tan solo se recomendarían otros tipos de transmisión de datos desde los sistemas de reserva y de control de salida relativos a los pasajeros y a la tripulación si cumplen con la legislación de los Estados miembros .

   Esta legislación debería procurar que toda restricción necesaria de los derechos y obligaciones que figuran en la Directiva 95/46/CE cumplan con el artículo 13 de la misma, y garantizar el amparo de las personas.

   Debería buscarse una perspectiva común de la UE.

5. Las transferencias de los datos que puedan ser considerados como delicados deberían realizarse con extrema precaución. Del mismo modo, al efectuar estas transferencias se presupone que se pueden ofrecer pruebas de que, en primer lugar, existen motivos de alto interés público para los Estados miembros, en segundo lugar las garantías adecuadas y, por último, que se requiere una legislación nacional o una decisión de la autoridad supervisora.

6. Si además se recomienda el acceso directo a los datos de los sistemas de reserva y de control de salida por parte del Servicio de Aduanas y el Servicio de Inmigración y Naturalización de los EE.UU., estas autoridades se comprometen a garantizar el respeto a la Directiva en su totalidad.

7. El sistema debería negociarse con las autoridades estadounidenses. En particular, los debates deberían centrarse en: aclarar y definir los objetivos, las finalidades y los receptores de los datos; las categorías de los datos que puedan transferirse, habida cuenta de estas explicaciones, y las condiciones y garantías que rodean al tratamiento de datos personales, en particular su envío a las autoridades federales de los EE.UU. (y, si este se produce, limitarlo a autoridades de las fuerzas de seguridad).

8. Debería adoptarse una perspectiva global para tratar la transferencia de datos personales por parte de las compañías aéreas a los Estados Unidos. En primer lugar, sería necesario tener en cuenta otras transferencias, existentes o planeadas, a dicho país. Sería especialmente necesario incorporar el concepto de tercer pilar. Esencialmente, las transferencias de datos a las autoridades públicas de terceros países por razones de orden público en este país deberían ser entendidas en el contexto de los mecanismos de cooperación establecidos por medio del tercer pilar (cooperación judicial y policial). Asimismo, estos mecanismos deberían estar estrechamente relacionados con las garantías de la protección de los datos transferidos[22]. Parece resultar importante para el buen funcionamiento de los mecanismos de cooperación basados en el tercer pilar que no se esquiven pasando, en su lugar, por el primer pilar. Por último, la solución a la que se lle gó para las transferencias de datos a los Estados Unidos podría resultar apropiada para servir de modelo a las transferencias que se realizan a terceros países distintos a través de APIS.

Hecho en Bruselas, a 24 de octubre de 2002

Por el Grupo de trabajo

Stefano RODOTA

Presidente

[22] Los Estados miembros exportan datos personales para lograr la cooperación judicial y policial. Europol está transfiriendo los datos para examinar los acontecimientos del 11 de septiembre de 2001 como parte de un procedimiento excepcional, y se están manteniendo conversaciones para establecer acuerdos de cooperación de manera estable, de acuerdo con los requisitos del Convenio Europol (artículo 18). Véase asimismo la Decisión Eurojust (artículo 27) y, por último, las negociaciones que en este momento se están manteniendo en torno al artículo 38 del Tratado.

Consejo de Europa

Comité de Ministros

Recomendación (2002)9
Del Comité de Ministros a los Estados miembros sobre la protección de datos personales recogidos y tratados a efectos de seguros

(Adoptada por el Comité de Ministros el 18 de septiembre de 2002 durante la 808ª reunión de Delegados de Ministros)

Preámbulo

El Comité de Ministros, al amparo del Artículo 15.*b* del Estatuto del Consejo de Europa,

1. Considerando que la finalidad del Consejo de Europa es realizar una unión más estrecha entre sus miembros;

2. Reconociendo los Principios generales relacionados con la protección de datos del Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal (STE Nº 108), y en concreto el Artículo 6, que dispone que datos personales clasificados como sensibles no podrán ser objeto de tratamiento salvo que la legislación proporcione las garantías oportunas;

3. Teniendo en cuenta el hecho que el tratamiento automatizado de datos personales a efectos de seguros es cada día más extendido, no sólo para la elaboración, formalización, implantación y finalización de contratos de seguro sino también para facilitar la gestión racional y económica de seguros y luchar contra el fraude;

4. Teniendo en cuenta que el seguro se otorga por distintas entidades financieras, especialmente por compañías de seguros;

5. Convencidos de la importancia que la calidad, integridad y disponibilidad de sus datos personales suponen para los Asegurados;

6. Observando que prácticamente la población entera de los Estados miembros es objeto de uno o más contratos de seguro, y que por este motivo los profesionales de seguros disponen de un volumen importante de datos personales, algunos de los cuales son de categoría sensible;

7. Convencidos de la conveniencia de regular la recogida y tratamiento de datos personales a efectos de seguros, de garantizar su carácter confidencial, la seguridad de los datos y garantizar que el uso que se haga de los datos respete los derechos y las libertades fundamentales, en concreto el derecho a la intimidad;

8. Teniendo en cuenta que la movilidad de las personas y la globalización de mercados y actividades comerciales requieren una transferencia internacional de información también en el sector de seguros y requieren protección de datos equiparable en todos los Estados miembros del Consejo de Europa,

Recomienda a los Gobiernos de los Estados miembros que:

1. adopten las medidas necesarias para garantizar que los Principios contenidos en el Anexo de la presente Recomendación se reflejen en sus leyes y en la práctica;

2. difundan ampliamente los Principios contenidos en el anexo de esta Recomendación entre las personas, autoridades públicas y organismos públicos o privados que recogen y tratan datos personales a efectos de seguros así como entre los organismos competentes en materia de la protección de datos;

3. fomenten la aceptación e implantación de los Principios contenidos en el anexo de esta Recomendación, notablemente mediante la adopción de provisiones legales o el fomento de la redacción de un código deontológico.

Anexo a la Recomendación Rec(2002)9

1. Definiciones

A efectos de la presente Recomendación:

a. «Datos personales» significa toda información sobre una persona física identificada o inidentificable («el interesado».) La persona física no tendrá la consideración de «identificable» si la identificación requiere tiempo y labor irrazonables.

b. «Datos sensibles» significa datos que revelan la raza de origen, opiniones políticas, creencias religiosas u otras creencias así como datos personales sobre la salud y vida sexual de la persona. Información sobre procedimientos penales y condenas y otra información definida como sensible según la legislación nacional tendrán también la consideración de datos sensibles.

c. «A efectos de seguros» comprende cualquier operación relacionada con la recogida y tratamiento de datos personales requeridos para cubrir un riesgo, en concreto mediante una póliza o contrato de seguro.

d. «Tratamiento» significa cualquier operación o conjunto de operaciones efectuadas parcial o totalmente mediante procedimientos automatizados y aplicadas a datos personales, como grabación, conservación, modificación, extracción, consulta, utilización, comunicación, cotejo o interconexión, así como su borrado o destrucción.

e. «Comunicación» significa la acción de poner datos personales a la disposición de terceros, con independencia de los medios o formatos utilizados.

f. «Responsable del Tratamiento» significa la persona física o jurídica, autoridad pública, servicio, o cualquier otro organismo que sólo o conjuntamente con otros, determine los fines y los medios utilizados en la recogida y tratamiento de datos personales.

g. «Encargado del Tratamiento» significa la persona física o jurídica, autoridad pública, servicio, o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

2. Ámbito

2.1. La presente Recomendación será de aplicación a datos personales recogidos y tratados a efectos de seguros. No se aplica a la recogida y tratamiento de datos personales a efectos de la seguridad social.

2.2. Se recomienda a los Estados que amplíen el ámbito de la presente Recomendación al tratamiento no-automatizado de datos personales a efectos de seguros.

2.3. Se prohíbe el tratamiento de datos personales mediante medios no automatizados con el fin de no tener que aplicar los Principios de la presente Recomendación.

2.4. Los Estados miembros podrán ampliar la aplicación de los Principios establecidos en la presente Recomendación a la recogida y tratamiento de datos sobre grupos de personas, asociaciones, fundaciones, empresas, corporaciones y cualquier otra entidad formada directa o indirectamente de personas físicas, con independencia del carácter jurídico de tales entidades.

2.5. Los Estados miembros podrán ampliar la aplicación de los Principios establecidos en la presente Recomendación a la protección de datos personales utilizados a efectos de la seguridad social.

3. Respeto de la intimidad

3.1. El respeto de los derechos y de las libertades fundamentales, en concreto el derecho a la intimidad, tiene que ser garantizado en el momento de recoger y tratar datos personales a efectos de seguros.

3.2. Las personas con acceso a datos personales en el transcurso de una actividad de seguros tendrán que ser sujetas, de acuerdo con la legislación y la práctica nacionales, a las reglas de confidencialidad. Además, la recogida y el tratamiento de datos de carácter sanitario sólo podrán realizarse por profesionales sanitarios o de acuerdo con reglas de secreto equiparables a las de aplicación a los profesionales de la sanidad o con garantías igualmente eficaces establecidas por la legislación nacional.

4. Recogida y tratamiento de datos personales a efectos de seguros

Condiciones fundamentales para la recogida y tratamiento de datos personales

4.1. La recogida y tratamiento (incluyendo la comunicación) de datos personales tienen que realizarse de una forma legítima y honesta y con finalidades lícitas y concretas.

Los datos personales deberían ser:

— adecuados, pertinentes y no excesivos en relación con las finalidades para las que se hayan obtenido o para las que recibirán tratamiento adicional.

— exactos y en su caso puestos al día.

Fuentes de datos personales

4.2. Los datos personales recogidos y tratados a efectos de seguros, en principio, deberían ser obtenidos del interesado o de su representante legal.

Legalidad

4.3. Datos personales pueden ser recogidos y tratados a efectos de seguros:

a. cuando la Ley lo prevea;

b. para la formalización de un contrato de seguro del que el interesado es una parte o parar la redacción de una póliza a solicitud del interesado;

c. cuando el interesado o su representante legal u otra persona u organismo acorde con la Ley hayan dado su consentimiento según lo establecido en el apartado 6; o

d. cuando los datos sean necesarios para el desarrollo de los intereses legítimos del responsable del tratamiento siempre que los intereses del afectado no prevalezcan sobre los del responsable del tratamiento.

Finalidad

4.4. Sujeto a las provisiones de los Principios 4.6 al 4.8, 8.1 y 13.1, los datos personales sólo pueden ser recogidos y tratados con la finalidad de:

a. la redacción y emisión de pólizas de seguro;
b. el cobro de primas y presentación de otras facturas;
c. la liquidación de siniestros o la realización de otras prestaciones;
d. el reaseguro;
e. el coaseguro;
f. la prevención, detección y/o persecución del fraude en seguros;
g. la justificación, persecución o defensa de una reclamación legal;
h. el cumplimiento de otra obligación específica legal o contractual;

i. la prospección de nuevos mercados de seguro;
j. le gestión interna;
k. actividades actuariales.

Los datos no podrán recibir tratamiento adicional con finalidades incompatibles con el motivo original de su recogida.

Hijos sin nacer

4.5. Los datos personales concernientes hijos sin nacer deberían gozar de una protección equiparable a la de los datos personales de un menor.

Siempre que la legislación nacional no disponga lo contrario el titular de las responsabilidades de tutela puede actuar como la personal legalmente facultada para actuar en nombre del hijo sin nacer, con éste teniendo la consideración de un interesado.

Datos sensibles

4.6. La recogida y tratamiento de datos sensibles deberían estar prohibidos salvo que se realicen para una de las finalidades expuestas en los Principios 4.4, 4.8, 8.1 y 13.1, y:

a. el interesado o su representante legal u otra persona u organismo acorde con la Ley hayan dado su consentimiento según lo establecido en el apartado 6; o

b. estén permitidos por la Ley y

i. sujeto a las garantías oportunas el tratamiento sea necesario para que el responsable del tratamiento cumpla con sus otras obligaciones legales o contractuales; o

ii. el tratamiento sea necesario para justificar, perseguir o defender una reclamación legal; o

iii. 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.

c. se permiten la recogida y tratamiento, sujeto a las garantías oportunas, cuando sean necesarios para la salvaguarda de un interés público importante y la Ley lo prevea o en virtud de una decisión de una autoridad acorde con lo previsto en el Principio 15.1.

Datos penales

4.7. En derogación parcial del Principio 4.6, la recogida y tratamiento de datos concernientes procedimientos penales y condenas podrán realizarse a efectos de seguros sólo cuando la legislación nacional establezca garantías especificas y adecuadas y los datos sean necesarios para combatir el fraude en el seguro, dar cobertura de seguro, o liquidar un siniestro o realizar otra prestación del seguro.

Marketing Directo

4.8. Siempre que el interesado haya sido informado y no haya presentado objeción, el responsable del tratamiento podrá utilizar, a efectos de marketing y promoción de su gama de servicios, los datos recogidos y tratados a efectos de seguros. No obstante, si el tratamiento concierne datos sensibles se requerirá el consentimiento explícito del interesado siempre que esto no sea contrario a la legislación nacional.

El interesado debería ser informado del hecho de que si deniegue su consentimiento o presente objeción a la utilización de sus datos a efectos de marketing, tal circunstancia no afectará a la decisión sobre la prestación o no de cobertura de seguro o la continuidad de cobertura ya vigente.

5. Información a disposición del interesado

5.1. Los interesados tendrán que ser informados de lo siguiente:

a. la finalidad o las finalidades con que los datos se tratan o se tratarán;

b. la identidad del responsable del tratamiento;

c. cualquier otra información necesaria para garantizar que el tratamiento sea justo, como:

- las categorías de los datos recogidos o a recoger;
- las categorías de las personas u organismos que puedan recibir los datos y las finalidades de la comunicación
- la posibilidad, si existe, de denegación de consentimiento o la retirada de consentimiento por parte del interesado y las consecuencias de tal retirada;
- las condiciones en que los derechos de acceso y rectificación pueden ejercerse;
- las personas naturales u organismos de los que se recogen o se recogerán los datos;

— el carácter obligatorio o voluntario de la contestación a las preguntas objeto de la recogida y las consecuencias de una respuesta incorrecta en relación con la persona.

5.2. Cuando los datos personales se obtienen del interesado el responsable del tratamiento debería facilitar al interesado la información relacionada en el Principio 5.1 anterior, al más tardar en el momento de la recogida, salvo que el interesado ya haya sido informado.

5.3. Cuando los datos personales no se obtienen del interesado el responsable del tratamiento debería facilitar al interesado la información relacionada en el Principio 5.1 en el momento de su registro, o si está prevista la comunicación de los datos a un tercero, al más tardar en el momento en que los datos se comuniquen por primera vez.

La obligación de informar al interesado no es de aplicación cuando:

a. el interesado ya haya sido informado;

b. resulte imposible facilitar la información o supondría esfuerzos desproporcionados;

c. el tratamiento o comunicación de datos a efectos de seguros estén explícitamente previstos en la legislación nacional.

En los casos planteados en *b* y *c*, las garantías oportunas tendrán que ser establecidas.

5.4. La información para el interesado tiene que ser procedente y adaptada a las circunstancias.

5.5. Si los interesados no tienen capacidad legal y no pueden tomar sus propias decisiones libremente, y si las normas nacionales no permiten que actúen en nombre propio, la información tiene que ser facilitada a las personas legalmente capacitadas para actuar en nombre de dichos interesados.

5.6. La provisión de datos a los interesados podrá ser restringida si la ley lo permite y si la restricción es necesaria para la prevención, investigación o juicio de un delito o para garantizar los derechos y las libertades de otras personas.

6. Consentimiento

6.1. Cuando se solicita el consentimiento a los interesados su consentimiento tendrá que ser prestado de una manera libre, específica e informada. Además tendrá que ser inequívoco, o en el caso de datos sensibles, explícito.

No obstante pueden existir circunstancias en que las normas nacionales no permiten que el consentimiento se considere suficiente justificación de la legalidad de la recogida o tratamiento.

6.2. Cuando los datos personales corresponden a personas que no tienen capacidad legal y la legislación no permite que el interesado actúe en nombre propio, el consentimiento de su representante legal o una autoridad u otra persona u organismo designado por ley será requerido.

6.3. Si, de acuerdo con el Principio 5.5 anterior, los interesados sin capacidad legal han sido informados del propósito de recoger y tratar datos sobre sus personas, sus deseos deberían ser tenidos en cuenta, siempre que no sea contrario a la legislación nacional.

7. Recogida y tratamiento por encargados de tratamiento

7.1. Según las disposiciones de las normas nacionales los responsables del tratamiento podrán contratar la recogida y tratamiento de datos personales para una finalidad determinada, en la medida en que estén autorizados a recoger y tratar estos datos, y con la condición que el encargado de tratamiento se compromete a actuar exclusivamente de acuerdo con las instrucciones del responsable de tratamiento y a respetar las disposiciones de las normas nacionales que implantan el Capítulo11del anexo de la presente Recomendación.

7.2. Los responsables del tratamiento tendrán que elegir encargados del tratamiento que ofrecen suficientes garantías en lo que se refiere a los aspectos técnicos y organizativos del tratamiento a realizar. Tendrán que vigilar el cumplimiento de las garantías y en concreto que el tratamiento se realice acorde con sus instrucciones.

7.3. La recogida y tratamiento de datos personales por encargados del tratamiento deberían regirse mediante un contrato o instrumento legal que vincule el encargado al responsable, estipulando que el encargado sólo actuará dentro del marco de referencia establecido por el responsable y las disposiciones de las normas nacionales que rigen las obligaciones de encargados.

8. Comunicación de datos para otros fines

8.1. Los datos personales sólo podrán comunicarse para fines distintos de los establecidos en el apartado 4.4 cuando:

a. la legislación nacional así lo permita y constituya una medida necesaria en una sociedad democrática destinada a la prevención, investigación y juicio de delitos o para garantizar otro interés público de importancia, o

b. los interesados o sus representantes legales o una autoridad u otra persona u organismo competente hayan prestado su consentimiento en los términos previstos en el apartado 6; o

c. la comunicación se realice a efectos de marketing directo, siempre que el interesado haya sido informado y no se haya opuesto. No obstante, el consentimiento explícito del interesado debería exigirse si los datos son de carácter sensible según lo previsto en el apartado 6; o

d. los datos sean necesarios para el desarrollo de los intereses legítimos del responsable del tratamiento, siempre que los intereses del interesado no prevalezcan sobre los mismos. No obstante, el consentimiento explícito del interesado debería exigirse si los datos son de carácter sensible según lo previsto en el apartado 6.

9. Decisiones individuales automatizadas

9.1. Las decisiones de seguros que tengan una influencia legal sobre los interesados o les afecten de forma significativa, no deberían tomarse exclusivamente en función del tratamiento automatizado de datos destinado a valorar ciertos aspectos personales de las personas según criterios previamente establecidos o resultados de la estadística.

9.2. No obstante, tales decisiones sí pueden tomarse si satisfacen una solicitud realizada por los interesados con vistas a la formalización o ejecución de un contrato de seguro, o si los interesados tienen la facultad de presentar su punto de vista con el fin de garantizar la protección de sus intereses legítimos. Tales decisiones también pueden tomarse si están permitidas por una ley que protege los intereses legítimos del interesado.

10. Derechos de acceso y rectificación

10.1. Todos los interesados deberían poder solicitar confirmación sobre si sus datos se procesan o no, y recibir en un formato legible todos los datos concernientes su persona, así como, como mínimo, información sobre las finalidades del tratamiento, las categorías de los datos que se traten, los destinatarios o categorías de destinatarios a los que se comunicarán los datos y la fuente de los datos. Además, deberían ser informados, previa solicitud, de la lógica subyacente del tratamiento automatizado de datos que les conciernen, al menos en el caso de decisiones individuales automatizadas.

10.2. Los derechos de los interesados de obtener datos sobre sus personas no serán restringidos salvo que la ley lo permita y la restricción sea necesaria para:

a. la prevención, investigación o juicio de un delito;

b. garantizar los derechos y libertades de los interesados o de otras personas.

En todo caso el derecho de acceso sólo podrá ser restringido mientras el motivo de la restricción siga vigente.

10.3. Los interesados deberían tener el derecho de poder hacer modificar, bloquear o suprimir sus datos según procede cuando dichos datos hayan sido recogidos o tratados en violación de las normas nacionales que incorporan los Principios de la presente Recomendación, y en concreto cuando los datos resulten ser inexactos, excesivos o impertinentes.

10.4. Los motivos de la restricción de derechos de acceso, rectificación, bloqueo o supresión tendrán que comunicarse por escrito. Cuando se restringen los derechos del interesado de acceso, rectificación, bloqueo o supresión, el interesado tendrá que ser informado de su derecho de solicitar a la autoridad competente verificación de la legalidad del tratamiento.

10.5. Terceras personas que hayan recibido datos personales tendrán que ser informadas de la rectificación, borrado o bloqueo salvo que esto resulte claramente irrazonable o inviable.

10.6. Los responsables del tratamiento deberían comunicar a intervalos razonables y sin demora o coste excesivos a las personas quienes ejercen el derecho de acceso a datos personales referentes a ellas, así como cualquier información mencionada en el Principio 10.1 a la que se solicita acceso.

11. Seguridad de datos

11.1. Las medidas oportunas de índole técnico y organizativo deberían adoptarse para proteger datos personales —de acuerdo con las provisiones de la legislación nacional que implantan los Principios de esta Recomendación— contra la destrucción accidental o ilícita, pérdida accidental, así como contra el acceso no autorizado, modificación o comunicación o cualquier otra forma de tratamiento ilícito.

Dichas medidas deberían garantizar un nivel adecuado de seguridad, teniendo en cuenta por un lado el estado técnico del arte y por otro lado la naturaleza sensible de datos recogidos y tratados a efectos de seguros y la valoración de riesgos potenciales. Estas medidas deberían ser revisadas periódicamente.

11.2. Para garantizar especialmente la confidencialidad, integridad y disponibilidad de datos tratados así como la protección de los interesados el responsable del tratamiento debería adoptar las medidas oportunas para:

a. evitar el acceso de cualquier persona no autorizada a las instalaciones utilizadas para el tratamiento de datos personales (control en la entrada de las instalaciones);

b. evitar que personas no autorizadas lean, copien, modifiquen o retiren medios de datos (control de medios de datos);

c. evitar la entrada no autorizada de datos en el sistema informático así como cualquier consulta, modificación o supresión no autorizadas de datos personales memorizados (control de memoria);

d. evitar que personas no autorizadas utilicen sistemas automatizados de tratamiento de datos mediante equipos de transmisión de datos (control de utilización);

e. con vistas a, por un lado, acceso selectivo a datos, y por otro lado, la seguridad de los datos personales, garantizar que como regla general el diseño del tratamiento permita la diferenciación entre:

— medios de identificación y datos referentes a la identidad de personas,
— datos administrativos,
— datos sensibles (control de acceso);

f. garantizar la posibilidad de conocer y verificar las personas u organismos que pueda recibir datos personales a través de equipos de transmisión de datos (control de comunicación);

g. garantizar que sea posible verificar e identificar, *a posteriori,* las personas que hayan tenido acceso al sistema, los datos introducidos en el sistema informático así como las fechas de tal acceso o introducción de datos (control de introducción de datos);

h. evitar la lectura, reproducción, modificación o supresión no autorizadas de datos personales durante la comunicación de datos personales y el transporte de medios de datos (control de transporte);

i. salvaguardar datos mediante la realización de copias de seguridad (control de disponibilidad).

11.3. Los responsables del tratamiento, de acuerdo con las normas nacionales, deberían establecer un reglamento interno adecuado que respeta los Principios correspondientes de esta Recomendación.

11.4. Cuando procede los responsables del tratamiento deberían designar una persona independiente responsable de la seguridad de los sistemas informáticos y protección de datos capacitada para asesorar sobre estas materias.

12. Transferencia internacional de datos

12.1. Los Principios de esta Recomendación son de aplicación a la transmisión entre países de datos personales recogidos y tratados a efectos de seguros.

12.2. La transmisión internacional de datos personales a un Estado que haya ratificado el Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal (STE No. 108), y cuya legislación establezca al menos protección de datos equiparable no debería ser sometida a condiciones especiales en relación con la protección de la intimidad.

12.3. No debería imponerse restricción sobre la transmisión internacional de datos a un Estado que no haya ratificado el Convenio pero cuya legislación sí garantice un nivel adecuado de protección.

12.4. Salvo que las normas nacionales establezcan lo contrario la transmisión internacional de datos a un Estado que no garantice un nivel adecuado de protección no debería realizarse, excepto cuando:

a. el interesado haya prestado su consentimiento según lo previsto en el apartado 6, o,

b. se hayan adoptado medidas, incluidas las de carácter contractual, necesarias para respetar las disposiciones de las normas nacionales que implantan los Principios del Convenio y de esta Recomendación y el interesado tenga la facultad de presentar objeción a la transmisión.

13. Conservación de datos

13.1. Cuando los datos personales ya no sean necesarios para la consecución de las finalidades para las que se recogieron y se trataron deberían ser borrados. Este principio es de aplicación también al caso de una decisión de denegar cobertura de seguro. No

obstante si los datos debiesen ser conservados a efectos de investigación científica o la estadística u otros fines previstos por la Ley, deberían ser conservados separadamente y accesibles sólo para dichos fines y sujetos a las garantías oportunas.

13.2. En el momento de establecer la duración del período de conservación de datos se tendrán en cuenta especialmente la necesidad de guardar datos durante el tiempo requerido a efectos de defensa en procedimientos legales o prueba de una transacción o justificación de una decisión negativa ante una solicitud de seguro.

14. Recursos

La legislación nacional debería establecer las sanciones y los recursos oportunos en caso de infracción de las disposiciones que incorporan los Principios establecidos en la presente Recomendación.

15. Garantía de respeto de los Principios

15.1. Los Estados miembros deberían conceder a una autoridad o más la responsabilidad de garantizar la aplicación imparcial e independiente de las normas nacionales que incorporen los Principios establecidos en la presente Recomendación.

15.2. La información siguiente debería publicarse oportunamente y estar a disposición de todos los interesados:

a. el nombre y domicilio del responsable de tratamiento y de su representante en su caso;

b. el motivo o los motivos del tratamiento;

c. la categoría o las categorías del interesado y de los datos;

d. el destinatario o categoría de destinatarios a los que los datos puedan revelarse

e. cualquier transferencia propuesta de datos a otros países.

Informe que contiene directrices para la protección de los individuos en relación con la recogida y procesado de datos mediante vigilancia por vídeo (2003)

Adoptado por el Comité Europeo de Cooperación Jurídica (CECJ) en su 78ª reunión (20-23 de mayo de 2003)

Introducción

Los comites de protección de datos del Consejo de Europa deseaban llamar la atención acerca de determinados aspectos de la vigilancia. El Grupo de Proyecto de Protección de Datos (CJ-PD) del Consejo de Europa solicitó por ello un asesor, el Dr. Giovanni BUTTARELLI (Secretario General de la Autoridad Italiana de Protección de Datos) que redactase un informe sobre la protección de datos en relación con las actividades de vigilancia. Este informe reconoció que cualquier estudio sobre vigilancia está vinculado a los avances tecnológicos de los medios de control y debe, por tanto, situarse en el contexto histórico. Por este motivo, se acordó destacar una lista de Directrices específicas para la vigilancia por vídeo, que deben tenerse en cuenta en relación con la vigilancia por vídeo.

Después de examinar las directrices y el informe del Sr. Buttarelli, el CJ-PD acordó reelaborar y especificar algunas de estas directrices, y redactó el texto que sigue.

Muchas entidades públicas y privadas han venido utilizando progresivamente sistemas de vigilancia en diferentes sectores para distintos fines, en particular para cotrolar el movimiento de personas y mercancías y el acceso a propiedades, así como acontecimientos, situaciones y conversaciones, ya sea mediante el teléfono, a través de redes electrónicas o un emplazamiento físico.

Los sistemas de vigilancia a menudo tienen como consecuencia la recogida de datos personales, aunque su recogida y/o almacenamiento no constituya, en ocasiones, el objetivo del controlador de los datos de vigilancia.

Una parte considerable de estas actividades se lleva a cabo mediante dispositivos de vigilancia por vídeo, que plantean problemas específicos por lo que se refiere a la protección de datos.

La información recogida durante las actividades de vigilancia por vídeo incluye a menudo datos (en forma de imágenes y sonido) que directa o indirectamente permiten la identificación de individuos y el control de su conducta. Además, los sistemas de vigilancia mediante vídeo convergen cada vez más con las tecnologías que plantean nuevas preocupaciones por lo que se refiere a la intimidad y protección de datos. Entre ellas se encuentran la grabación de sonidos, las redes informáticas inalámbricas y de alta velocidad empleadas para transferir imágenes; los sistemas de reconocimiento facial integrados con bases de datos informatizadas que puedan identificar y seguir a los individuos; y dispositivos de búsqueda bajo las ropas y a través de las paredes, por ejemplo, dispositivos de reconocimiento mediante calor o dispositivos de infrarrojos.

Las actividades de vigilancia mediante vídeo que llevan consigo el procesado de datos personales se encuentran dentro del ámbito de aplicación del Convenio para la Protección de los Individuos en relación con el Procesado Automático de Datos Personales del Consejo de Europa [ETS N.º 108] (en adelante, Convenio 108), que fue elaborado cuando se hizo patente que, para garantizar una protección jurídica eficaz de los datos personales, iba a resultar necesario desarrollar de forma más específica y sistemática la referencia general al respeto a la vida privada contenida en el Artículo 8 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales (en adelante, CEDH).

En diversas Recomendaciones del Consejo de Europa se establecen derechos y salvaguardas adicionales, en particular:

- Recomendación N.º R(87) 15, relativa al uso de datos personales en el sector policial;
- Recomendación N.º R(89) 2, relativa a la protección de datos personales utilizados con fines laborales;
- Recomendación N.º R(95) 4, relativa a la protección de datos personales en el sector de las telecomunicaciones;

Existen otras recomendaciones que, aunque no se refieren expresamente a la vigilancia por medio de vídeo, incluyen salvaguardas y normas que resultan relevantes en términos de protección de datos personales, al estar también relacionadas con la comunicación de datos y con los flujos de datos transfronterizos.

La vigilancia por medio de vídeo no está expresamente contemplada en estos instrumentos. En vista del aumento del empleo de la vigilancia por vídeo y de los avances tecnológicos en este campo, resulta necesario abordar esta cuestión.

Por ello, estas directrices amplian y especifican con mayor detalle las salvaguardas aplicables a los sujetos de los datos contenidas en las disposiciones de los instrumentos anteriores citados, por lo que se refiere al procesado de datos personales recogidos a través de la vigilancia por vídeo. Incluyen cualquier tipo de actividad de vigilancia por vídeo que permita (mediante equipos técnicos) la observación, recogida y/o almacenamiento sistemáticos de datos personalesrelacionados con uno o más individuos, en particular relacionados con su conducta, presencia y/o movimientos. Estas directrices deben incluir la observación sistemática, con independencia de que sea permanente o con ocasión de un acontecimiento específico, de que los datos personales sean procesados en su totalidad o en parte por medios automáticos, y de que formen parte de un sistema de archivos o constituyan un procesado sistemático no automático.

Algunas directrices anticipan nuevas posibilidades de la tecnología de la información que van a permitir el acceso fácil y la corrección sin revelar los datos personales de terceros.

Hay que llamar la atención sobre el hecho de que, en la medida en que estas directrices contienen salvaguardas de los derechos y libertades fundamentales de todos, y en particular el derecho a que se respete la intimidad, tal y como se establece en los artículos 5, 6 y 8 del Convenio 108 y en el artículo del CEDH, las excepciones a tales derechos, de conformidad con el artículo 9 del Convenio 108, que fueron redactadas sobre la base del artículo 8 del CEDH, son posibles cuando estén establecidas por ley y constituyan una medida necesaria en una sociedad democrática en interés de:

- Proteger la seguridad del estado, la seguridad pública, los intereses monetarios del Estado o la supresión de delitos.
- Proteger al sujeto de los datos, o lo derechos y libertades de otros.

La finalidad de estas directrices es darles la mayor divulgación posible entre los individuos que puedan ser objeto de vigilancia por medio de vídeo, así como entre los usuarios de sistemas, dispositivos y técnicas de vigilancia por vídeo. También van dirigidas a los estados miembros, fabricantes, comerciantes, proveedores de servicios y de acceso e investigadores, con el fin de desarrollar software y tecnologías que tengan más en cuenta a los derechos fundamentales de los sujetos de los datos en el que se refiere a la vigilancia mediante vídeo. Los Estados miembros del Consejo de Europa deben garantizar que estos principios rectores se apliquen de la forma más coherente posible.

Estas directrices pueden servir también como marco para otras actividades de vigilancia que no estén basadas en el uso de dispositivos de vigilancia por vídeo.

Directrices

Cualquier actividad de vigilancia mediante vídeo debe ser llevada a cabo adoptando las medidas que sean necesarias con el fin de garantizar que esta actividad respete los principios relativos a la protección de los datos personales, en particular:

1. Garantizando que se lleve a cabo de una forma leal y legalmente permitida, para fines legítimos, específicos y explícitos. Los datos personales recogidos a través de la vigilancia por vídeo no deben ser procesados después de una forma incompatible con los fines para los que fueron recogidos.

2. Utilizando la vigilancia mediante vídeo solamente cuando, en función de las circunstancias, el fin no pueda ser alcanzado adoptando medidas que interfieran menos en la intimidad, siempre que dichas medidas alternativas no supongan un coste desporporcionado.

3. Haciendo uso de la vigilancia mediante vídeo de forma adecuada, pertinente y no escesiva en relación con los fines determinados y específicos que se persiguen en cada caso individual en que exista una necesidad acreditable, con el fin de evitar culaquier infracción involuntaria e injustificada de los derechos y libertades fundamentales del sujeto de los datos, por ejemplo, la libertad de movimiento, y para garantizar en particular el respeto a su intimidad, incluso en lugares públicos.[1]

4. La vigilancia mediante vídeo debe realizarse de una forma que no haga reconocibles a las personas grabadas cuando la finalidad del procesado no requiera su posible identificación.

5. Impidiendo que los datos recogidos sean indexados, comparados o conservados de forma innecesaria. Cuando se demuestre la necesidad de guardar los datos, éstos deben ser eliminados tan pronto como ya no resulten necesarios para la finalidad determinada y específica que se persiga.

6. No llevando a cabo actividades de vigilancia mediante vídeo cuando el procesado de los datos pueda redundar en una discriminación contra determinados sujetos de datos o grupos de sujetos de datos exclusivamente como consecuencia de sus opiniones políticas, creencias religiosas, salud o vida sexual, origen racial o étnico.

---

[1] Por ello, se invita a los responsables de estos sistemas a que evalúen e que medida están adaptados los sistemas de vigilancia por video a sus necesidades de información en relación con la situación geográfica de las cámaras (qué áreas de la ciudad, qué calles y por qué), y a que elijan la tecnología que debe emplearse conforme a estas misma necesidades (definición de imagen, capacidad de zoom, minituarización de cámara, etc,) sin usar medidas excesivas.

7. Haciendo claramente discernible de una forma adecuada que se está llevando a cabo la vigilancia mediante vídeo, su finalidad y la identidad del controlador[2] o informando previamente de lo anterior al sujeto de los datos. Debe darse otra información adicional al sujeto de los datos[3], en función de las circunstancias específicas, cuando dicha información resulte necesaria para garantizar un procesado leal de sus datos personales y no se ponga en peligro la finalidad de la vigilancia.

8. Garantizando que, durante el período de almacenamiento el sujeto de los datos tenga derecho de acceder a los datos y, en su caso, derecho de rectificación, bloqueo y/o borrado de los mismos, salvo que esto suponga un esfuerzo desproporcionado.

9. Adoptando todas las medidad técnicas u organizativas necesarias para salvaguardar la integridad de la información recogida.[4]

10. En caso de almacenamiento por parte de la policía, como consecuencia de la vigilancia por vídeo, de datos personales mediante procedimientos automáticos, habrá que tener en cuenta además los principios de la Recomendación R(87) 15, relativa al uso de los datos personales en el sector policial.

11. Limitando el uso de los sistemas de vigilancia por vídeo en el lugar de trabajo a exigencias organizativas o de producción, o a fines de seguridad en el trabajo. Este sistema no debe tener por finalidad la vigilancia sitemática de la calidad y cantidad del rendimiento del individuo en el lugar de trabajo.

    Los empleados y sus representantes deben ser informados o consultados antes de la introducción o adaptación de un sistema de vigilancia por vídeo. Cuando el procedimiento de consulta revele la posibilidad de que se infrinja el derecho de los empleados a que se respete su intimidad y dignidad humana, deberá obtenerse su consentimiento[5]. En caso de demanda judicial o de reconvención, los empleados deben poder fundamentarlas en la grabación efectuada.

---

[2] En algunos casos, la finalidad y la identidad del controlador están claros en función de las circunstancias. No obstante, en determinados casos concretos (por ejemplo, gestión del tráfico), puede no resultar viable facilitar de antemano la identidad del controlador.

[3] La información que debe darse al sujeto de los datos puede incluir también especificaciones técnicas del sistema elegido.

4 Esto reviste una especial importancia en casos de digitalización, dado que la alteración de datos no puede detectarse fácilmente. La información recogida únicamente debe modificarse por motivos adecuados y justificados, la información recogida modificada debe etiquetarse como tal y la información original debe conservarse.

[5] Por ejemplo, esta conformidad pueden presentarla, de acuerdo con los correspondientes porcedimientos legales internos, los sindicatos o comités de empresa.

12. En caso de que se graben y guarden datos personales, esto deberá realizarse, en la medida de lo posible, de forma que permita a los sujetos de los datos ejercer su derecho de acceso, de acuerdo con la legislación de protección de datos, sin obtener información acerca de otras personas.