

**Grupo de Protección de las Personas en lo que respecta
al Tratamiento de Datos Personales**

Dictamen 3/99 relativo a

Información del sector público y protección de datos personales

**Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado
"La información del sector público: un recurso clave para Europa"
COM(1998) 585**

Aprobado el 3 de mayo de 1999

Dictamen 3/99 relativo a

INFORMACIÓN DEL SECTOR PÚBLICO Y PROTECCIÓN DE DATOS PERSONALES

INTRODUCCIÓN Y OBSERVACIONES PRELIMINARES:

1. La Comisión Europea sometió a consulta pública un Libro Verde sobre "La información del sector público: un recurso clave para Europa"¹. El principal objetivo de este Libro Verde es promover un debate sobre cómo hacer más accesible a los ciudadanos y a las empresas la información que posee el sector público, así como sobre la posible necesidad de armonizar las normas nacionales en este ámbito. Este documento parece ampliamente inspirado por la reivindicación de entidades privadas que desean disponer de un acceso al menor coste posible a la información pública e impugnan el mantenimiento de monopolios públicos en este ámbito.

Una de las cuestiones tratadas por el Libro Verde atañe a la disponibilidad de la información del sector público, es decir, de una categoría particular de datos llamados "públicos": aquellos que, estando en posesión de organismos del sector público, se harían públicos en virtud de normas o de un uso² cuyo fundamento implícito o explícito puede residir en una voluntad de transparencia del estado respecto a sus ciudadanos³.

No se ignora en este documento la protección de los datos personales, aunque aparentemente no constituye su principal razón de ser.

El apartado 111 (III. 7, página 17) menciona explícitamente que la Directiva 95/46/CE sobre protección de datos personales⁴ "establece normas vinculantes tanto para el sector público como para el privado y [...] es de obligado cumplimiento en los casos de datos personales en manos del sector público.

El apartado 114 destaca que "El crecimiento de la sociedad de la información puede plantear nuevos riesgos para la intimidad del particular si se facilita el acceso a los registros públicos en formato electrónico (especialmente en línea y a través de Internet) y en grandes cantidades".

Con todo, el Libro Verde en su conjunto suscita varias ambigüedades sobre la fuerza de esta convicción.

¹ COM(1998) 585, disponible en la siguiente dirección: <http://www.echo.lu/legal/en/acces.html>.

² Parece poder hacerse una distinción entre la publicidad ordenada por una legislación, el acceso a la información autorizado por ley y situaciones en las que la cuestión de la publicidad o del acceso es consecuencia de un requerimiento formulado por particulares o empresas respecto al sector público sin que la regule una ley.

³ El presente dictamen no trata, pues, de la otra acepción - más amplia - del término «dato llamado "público"»: la que comprende el conjunto de los datos tratados por las administraciones públicas.

⁴ Directiva del Parlamento 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 pág. 31-51 Disponible en la dirección siguiente: <http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm>.

En primer lugar, la utilización (en la versión inglesa) del término “*publicly available*” (públicamente disponible) es propicia a la concepción de que los datos hechos públicos quedarían, así, disponibles para cualquier uso. Obsérvese que el principio de finalidad, pilar de nuestras legislaciones de protección de datos, se combina mal con el adjetivo “disponible”. Además el principio de la lealtad de la recogida - garantizado, entre otras cosas, por la exigencia de seguridad en el tratamiento de los datos - podría verse afectado por el hecho de que un dato se haga público de forma descuidada e irreflexiva. Por ello convendría que la expresión “*publicly available*” se sustituya por otra más apropiada e inequívoca (por ejemplo “*publicly accessible*”)

En segundo lugar, de la pregunta nº 7 (“Los problemas de intimidad ¿merecen especial atención en lo que atañe a la explotación de la información del sector público?”, página 17) se podría deducir que la recapitulación de los preceptos de la Directiva 95/46/CE no conduce tan firmemente como se habría podido imaginar a conclusiones precisas sobre este punto, al mismo tiempo que se precisa (apartado 111) que la Directiva 95/46/CE “consigue el equilibrio necesario entre el principio de acceso a la información del sector público y la protección de los datos personales”. Estas ambigüedades deberían desaparecer.

2. En este contexto, el presente dictamen tiene por objetivo alimentar la reflexión sobre la dimensión de la protección de los datos personales, esencial cuando se pretende facilitar el acceso a datos del sector público que se refieren a personas físicas. No pretende sin embargo ofrecer todas las respuestas a las cuestiones que plantea en cada caso la conciliación entre el objetivo de facilitar el acceso a los datos del sector público, fundada en la voluntad de reforzar la transparencia de los Estados respecto a los ciudadanos, y la protección de los datos personales, tal como se define en la Directiva 95/46/EC.

Este dictamen no tratará por tanto de las cuestiones planteadas por el Libro Verde que parecen sobrepasar la mera puesta a disposición de terceros de la información del sector público, como por ejemplo el punto de vista expresado en el apartado 56 (II 2, página 10) “la utilización de las nuevas tecnologías podrá aumentar considerablemente la eficacia de la **recogida de la información**. Proporciona a los entes públicos la posibilidad de compartir la información disponible, cuando ello sea conforme con las normas de protección de datos”.

Su objetivo es proporcionar, basándose en la Directiva 95/46/CE, así como en experiencias concretas recogidas con fines pedagógicos en el ámbito de los registros más conocidos de datos personales hechos públicos, un primer conjunto de puntos de referencia que conviene tener en cuenta cuando se toman decisiones concretas. Estos puntos de referencia y ejemplos concretos recogidos en distintos Estados miembros están destinados a ilustrar cómo deben considerarse en la sociedad de la información las normas de protección de datos cuando se trate de datos procedentes de registros públicos y a indicar algunas de las medidas de carácter técnico u organizativo que pueden contribuir (sin que por ello pretendan garantizar una protección sin fallas) a conciliar la publicidad de estos datos y el respeto de las disposiciones de protección de datos personales, sobre todo el de las relativas al principio fundamental en este tema, a saber, el principio de finalidad para la cual los datos se hacen públicos en el caso que aquí nos interesa.

I - LAS NORMAS DE PROTECCIÓN DE DATOS SE APLICAN A LOS DATOS PERSONALES HECHOS PÚBLICOS

La accesibilidad de las informaciones que dependen del sector público, sobre todo a través de la informatización preconizada por el Libro Verde, plantea el problema de saber de qué modo se utilizan estas informaciones. La solución no está en prohibir su utilización, la evolución de nuestras sociedades no va en ese sentido. Tampoco van en ese sentido nuestras legislaciones de protección de datos, garantes del acompañamiento de la informatización de la sociedad y no de su prohibición.

Por lo demás, afirmar la aplicabilidad de nuestras leyes de protección de datos a los datos personales hechos públicos, no es más que la expresión de una evidencia que deriva de los textos sobre protección de datos: un dato de carácter personal, incluso hecho público, sigue siendo un dato de carácter personal y goza, por lo tanto, de protección.

Esta afirmación implica necesariamente determinar cuál es la protección que se ofrece al dato de carácter personal hecho público. A este respecto, la Directiva 95/46/CE ya da algunas respuestas.

Directiva del Parlamento 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;

La Directiva permite tener en cuenta, en la aplicación de las normas que establece, el principio del derecho de acceso del público a los documentos administrativos⁵ así como otros elementos pertinentes para la discusión⁶.

Así el principio de finalidad exige que los datos personales se recojan para finalidades determinadas, explícitas y legítimas y no se traten posteriormente de manera incompatible con ellas.⁷ Este principio desempeña pues un papel central en la accesibilidad de datos personales en el sector público.

Conviene, sobre todo, determinar caso por caso en qué medida una ley exige o autoriza la publicación o el acceso por el público a datos personales: ¿contempla una accesibilidad íntegra e ilimitada en el tiempo, permite una utilización de esos datos con cualquier objetivo independientemente de la finalidad inicial o, al contrario, prevé la accesibilidad solamente a ciertas partes y/o una utilización vinculada a la finalidad para la cual el dato se hizo público? Por lo tanto, no existe una sola categoría de datos personales, destinados a hacerse públicos, que deba tratarse uniformemente desde el punto de vista de la protección de datos, sino que conviene más bien proceder a un análisis por grados en la delimitación de los derechos del

⁵ Véase el considerando 72. Conviene tener en cuenta para el debate que la Directiva no contiene definición del término “documentos administrativos”, pero que puede entenderse en un sentido amplio que permite cubrir al menos las “informaciones administrativas” previstas por el Libro Verde en su propuesta de clasificación de las informaciones (apartado 73 y siguiente, página 12).

⁶ Véase el artículo 10 y considerando 37 de la Directiva 95/46/CE sobre la conciliación del derecho a la intimidad con las normas que regulan la libertad de expresión. Véase también la Recomendación 1/97 del Grupo sobre “**Legislación sobre protección de datos y medios de comunicación**”, adoptada el 25.2.1997 (documento 5012/9, disponible en las 11 lenguas en la dirección indicada en nota 1).

⁷ Véase para mayor detalle la letra b) del apartado 1 del artículo 6 de la Directiva 95/46/EC.

individuo al que los datos se refieren y de los derechos del público a acceder a esa información. Aunque el acceso a los datos pueda ser público, puede estar sujeto a condiciones (como la justificación de un interés legítimo) y su explotación, con fines comerciales por ejemplo, o por los medios de comunicación, puede restringirse. Los ejemplos siguientes van a ilustrar estas cuestiones.

Es útil recordar aquí que independientemente de una eventual publicación de datos personales, la persona interesada tiene siempre derecho de acceso a sus datos y el derecho a exigir, cuando proceda, su rectificación o el borrado de datos cuyo tratamiento no se ajuste a lo dispuesto en la Directiva debido, sobre todo, a su carácter incompleto o inexacto⁸.

Cierto es que distintos preceptos de la Directiva hacen referencia explícita al carácter público de un dato. Dos de estos preceptos merecen ser citados con todos sus matices.

El artículo 18.3, que impone que los tratamientos se notifiquen a la autoridad de control, permite una excepción a esta obligación en caso de registros que, “en virtud de disposiciones legislativas o reglamentarias se destinen a información del público y estén abiertos a la consulta pública”. Aunque los considerandos 50 y 51 de la Directiva precisan que estas excepciones o simplificaciones no se aplican a los tratamientos cuyo único objetivo (1ª condición) sea mantener un registro destinado, de acuerdo con el derecho nacional, a la información del público (2ª condición) y que están abiertos a consulta pública o a cualquier persona que justifique interés legítimo (3ª condición), sin que el beneficio de tales excepciones exima al responsable del tratamiento de ninguna de las demás obligaciones que se derivan de la Directiva.

Por último, la letra f) del artículo 26, que constituye una excepción a la exigencia de un nivel adecuado de protección para los datos objeto de transferencia hacia terceros países cuando la transferencia no ofrezca ese nivel de protección siempre que se realice “a partir de un registro destinado a información del público”. Sin embargo, el considerando 58 de la Directiva limita el alcance de la transferencia precisando que no debe referirse a la totalidad de los datos ni a las categorías de datos contenidos en este registro y que, cuando proceda efectuarla, la transferencia sólo debe poder realizarse a petición de las personas con un interés legítimo.

Pero resulta claramente de estos preceptos y precisiones que si bien la protección de los datos personales no debe constituir un obstáculo al derecho de los ciudadanos a tener acceso a los documentos administrativos en las condiciones previstas por cada legislación nacional, la Directiva no pretende sin embargo privar de toda protección a los datos accesibles al público.

El debate referente a la cuestión de si es necesario armonizar las normas nacionales sobre el acceso a la información del sector público debe en cualquier caso tener en cuenta las normas armonizadas sobre protección de datos personales, así como de las medidas nacionales de transposición correspondientes.

⁸ Véase artículo 12 de la Directiva 95/46/EC.

Además de la misión de la Comisión de velar por la aplicación de la Directiva 95/46/CE, corresponderá al Grupo creado por el artículo 29 de la misma apreciar concretamente el alcance de las disposiciones nacionales adoptadas en su aplicación en los casos precisos que puedan revelar divergencias a escala nacional.⁹

B - Ejemplos de conciliación de las normas de la protección de los datos personales y del acceso a la información del sector público

Algunas legislaciones supeditan la difusión de la información del sector público a ciertas finalidades que pueden llevar, sea a prohibir el acceso a determinados datos, o a ponerle condiciones, sea a prohibir algunas formas de utilización de los mismos.

Ahora bien, la digitalización de las informaciones y las posibilidades de búsqueda en texto íntegro pueden, sin embargo, multiplicar *ad infinitum* las posibilidades de interrogación y selección, sin olvidar que la difusión por Internet aumenta los riesgos de captación y desvío de uso. Además, la aproximación a datos hechos públicos a partir de fuentes diferentes, cuando éstas se ponen a disposición del público, se ve facilitada en gran medida por la digitalización de los datos y permite, sobre todo, establecer perfiles sobre la situación o el comportamiento de los individuos¹⁰. También es conveniente prestar una atención especial al hecho de que, al poner así datos personales a disposición del público, se beneficia a las nuevas técnicas de «*data warehousing*» y «*data mining*». Estos métodos permiten recoger datos sin ninguna especificación *a priori* de la finalidad, y es sólo en fase de la explotación cuando se definen las distintas finalidades. Por lo tanto, es necesario tener en cuenta todo lo que es técnicamente posible hacer con los datos¹¹.

Esta es la razón por la que es conveniente comprobar, caso por caso, cuáles podrían ser las repercusiones negativas sobre el individuo antes de tomar cualquier decisión de difusión en

⁹ Véanse los artículos 29 y 30 de la Directiva 95/46/EC.

¹⁰ Convendría señalar que el uso de estas tecnologías confiere también al estado la posibilidad de establecer tales perfiles.

¹¹ Otro ejemplo: gracias al cotejo electrónico de dos bancos, se puede obtener más fácilmente informaciones negativas sobre tal o cual persona, por ejemplo: el cotejo del censo de población (si existe) y de los padrones electorales permite identificar a las personas que no tienen derecho de voto.

soporte digital. Según los casos, conviene, o bien decidir no difundir ciertos datos personales, o bien someter la difusión a la valoración de la persona en cuestión o a otras condiciones.

1 - Bases de datos de jurisprudencia:

El apartado 74 del Libro Verde (página 11) que hace particular referencia a los procesos judiciales para ilustrar el concepto de información fundamental para el funcionamiento de la democracia”, plantea una cuestión de fondo. En efecto, ¿se puede concebir que todos los juicios de todos los órganos jurisdiccionales estén disponibles en Internet sin perjuicio para las personas?

Instrumentos de documentación jurídica, las bases de datos de jurisprudencia pueden convertirse, si no se toman precauciones particulares, en ficheros de información sobre personas si se consultan, no para conocer una jurisprudencia, sino para obtener, por ejemplo, todas las decisiones judiciales que se refieren a una misma persona.

La Comisión de Protección de la Vida Privada (Bélgica), en un dictamen de 23 de diciembre de 1997, puso vigorosamente en evidencia que “la evolución tecnológica debe ir acompañada de una mayor contención en cuanto a la mención de la de identificación de las partes en los anales de jurisprudencia”. Propone que a falta de una completa omisión de la identificación de las partes, las decisiones judiciales accesibles al público en general no estén indexadas a partir del nombre de las partes, con el fin de impedir las búsquedas a partir de este criterio.

La Comisión de protección de datos personales italiana¹² prevé proponer a escala nacional que las partes tengan un derecho de oposición a la publicación de sus nombres respectivos en las bases de datos de jurisprudencia. Este derecho podría ejercerse en cualquier momento y tenerse en cuenta en las actualizaciones de bases de datos divulgadas en soporte magnético. El ejercicio de este derecho no tendría efectos retroactivos para las publicaciones en papel.

En Francia, el Ministerio de Justicia, que pretende difundir las bases de datos de jurisprudencia en Internet, impuso, en el pliego de condiciones, que las decisiones judiciales se hiciesen anónimas.

2 - Algunos textos oficiales:

La difusión de informaciones en Internet implica una plétora de información a escala mundial y una multiplicación de las fuentes. Este cambio de escala geográfico puede originar un riesgo específico. En efecto, la difusión de una información legítimamente pública en un país puede, a escala mundial, causar graves ataques a la intimidad o a la integridad física de las personas. Esto sucede, cuando, por ejemplo, las decisiones de naturalización son objeto de

¹² Garante per la protezione dei dati personali

publicación oficial obligatoria. Tal es el caso en Francia donde, siguiendo en este aspecto el dictamen de la Comisión Nacional de Informática y Libertades (CNIL), el gobierno francés, cuando el "Journal Officiel" se puso en Internet, excluyó estos textos de la difusión, con el fin de evitar a algunos nacionales que habían renunciado a su nacionalidad de origen el riesgo de incurrir en posibles represalias.

Podemos observar que, en algunos casos, la voluntad de transparencia de un Estado, y en particular de sus nacionales, puede adaptarse mal a la difusión a escala planetaria de tales informaciones.

3 - Otros ejemplos de difusión de datos personales hechos condicionalmente públicos con miras a proteger a la persona interesada:

Las condiciones de acceso a los datos personales contenidos en registros pueden ser muy variadas, según las normativas: por ejemplo, acceso parcial a los datos del registro, comprobación de un interés legítimo, prohibición de uso comercial.

En Alemania, todas las listas de candidatos a una elección federal deben contener nombre y apellido, profesión o situación, día, lugar de nacimiento y dirección. Sin embargo, en las listas hechas públicas antes del escrutinio por el responsable local o del Estado Federado encargado de la organización de las elecciones federales, el día de nacimiento se sustituye por el año de nacimiento.

En Italia, la legislación relativa al registro de empadronamiento que realiza cada municipio prevé la prohibición de comunicar datos a organismos privados y la obligación, por parte de cualquier administración que pueda solicitar la comunicación de datos, de aportar la prueba de un interés público pertinente.

En Francia, el padrón electoral es público a fin de poder auditar su regularidad. La ley permite la utilización con fines políticos por todos los candidatos y todos los partidos y prohíbe el uso comercial. No sería concebible, por tanto, que los padrones electorales pudieran difundirse por Internet.

Del mismo modo, en Francia, los datos personales contenidos en el catastro son públicos, pero está prohibido el uso comercial.

En Grecia, el sistema actual de catastro, organizado sobre la base de un registro alfabético de propietarios de bienes inmuebles, se sustituirá por un registro basado en la definición del bien inmueble, con el fin de impedir que las búsquedas se refieran a los conjuntos de bienes inmueble que pertenecen a una misma persona. Para tener acceso al catastro debe poderse justificar un interés legítimo.

II - LAS NUEVAS TECNOLOGÍAS PUEDEN CONTRIBUIR A CONCILIAR LA PROTECCIÓN DE DATOS PERSONALES Y SU PUBLICIDAD

Sin dejar de favorecer el acceso a los datos públicos, entre otras cosas mediante su "puesta en línea", las nuevas tecnologías y ciertas medidas administrativas de acompañamiento pueden facilitar el respeto de los principios esenciales de la protección de datos, como son el principio de finalidad, el de información y los derechos de oposición o de seguridad.

No obstante, la utilización de estas tecnologías no presenta una garantía absoluta contra el riesgo de abuso y desvío de principios de protección de datos personales tal como ya se ha descrito.

A - Las condiciones técnicas de acceso a la información del sector público deben contribuir al respeto del principio de finalidad

Habida cuenta de las condiciones de accesibilidad digital del público, es ciertamente muy difícil garantizar en la práctica la especificación de la finalidad, pero un uso ponderado y bien orientado de la técnica debería contribuir a lograr este objetivo. Conviene para ello comprobar y definir en cada caso las condiciones de interrogación. A este respecto, debería aplicarse el principio siguiente: "cualquiera puede acceder a cualquier dato individualmente, en las condiciones autorizadas, pero no a todos los datos en conjunto". La elección de los criterios de búsqueda que deben introducirse debe excluir cualquier abuso en situación normal. Conviene por otro lado comprobar si no es posible orillar «el obstáculo» obteniendo informaciones complementarias en otras fuentes.

Esta es la razón por la que la consulta en línea de bancos de datos puede ser objeto de restricciones con miras a prevenir el desvío de la finalidad para la cual se hacen públicos los datos. Estas medidas, adaptadas a cada caso, pueden consistir, por ejemplo, en limitar el campo de búsqueda o los criterios de interrogación.

Podemos observar que, en Francia, los extractos de partida de nacimiento son accesibles a cualquier persona que disponga de la identidad, la fecha y el lugar de nacimiento de una persona. El CNIL supeditó la consulta en línea de estos extractos a la condición de que la demanda en línea implique el conjunto de estas informaciones. La determinación de criterios restrictivos de interrogación de la base puede evitar la recogida masiva de este tipo de registros para fines comerciales respetando la finalidad de la accesibilidad.

En Francia también, el listín telefónico publicado en soporte telemático se podía consultar a partir de las primeras letras del nombre, lo que hacía más fácil su descarga completa y su utilización comercial contra la voluntad de algunos abonados que se oponían a este uso. Hacer imposible este tipo de búsqueda en Minitel e Internet permitió prevenir posibles desvíos de finalidad operados por este medio.

En los Países Bajos, los CD-ROM destinados a la difusión de la guía telefónica se concibieron de tal forma que se pudiese impedir la obtención del nombre y la dirección de

una persona sabiendo su número de teléfono (no es posible la interrogación de la base de datos a partir únicamente del campo *número de teléfono*).

Del mismo modo, las bases de datos relativas a los registros de empresas no deben poder interrogarse según el criterio del nombre de una persona, pues ello podría conducir a una búsqueda de todas las empresas en las que figura dicha persona.

B Promover la utilización de instrumentos técnicos que puedan impedir la captación automatizada de datos accesibles en línea

Se podría citar el protocolo de exclusión de los motores de investigación (The Robots Exclusion Protocol) que tiene por objeto impedir la indexación automatizada por un motor de búsqueda de la totalidad o una parte de las páginas de un sitio. En cualquier caso, estos métodos sólo podrán ser eficaces si se informa a los diseñadores de parajes y los internautas de su existencia y si los motores de búsqueda los respetan. Algunas sociedades editoras de motores de búsqueda declaran respetar este protocolo.

III. Utilización comercial

Inicialmente los datos personales en el sector público se recogían y se trataban con objetivos precisos y, en principio, sobre la base de una normativa. A veces la recogida era obligatoria, otras veces era una condición para acceder a un servicio público. El ciudadano interesado no espera inevitablemente que los datos que le conciernen se hagan públicos y se utilicen con fines comerciales. Esta es una de las razones por las cuales algunas legislaciones nacionales permiten el acceso a la información del sector público, prohibiendo, sin embargo, la utilización comercial de esa información, incluyendo los datos personales¹³.

Desde el punto de vista de la Directiva 95/46/CE¹⁴, se plantea la cuestión de saber si la utilización comercial debe considerarse como una finalidad incompatible con aquélla para la cual se recogieron inicialmente los datos y, en caso de que la respuesta sea afirmativa, la cuestión de saber bajo qué condiciones podría considerarse posible la utilización comercial.

Si se admite la publicación y la comercialización de la información del sector público¹⁵, es necesario respetar algunas normas y plantearse caso por caso la cuestión de cómo reconciliar efectivamente el respeto del derecho a la intimidad con los intereses comerciales de los agentes.

¹³ Véase Anexo 1 del Libro Verde: [Situación actual en los Estados miembros por lo que se refiere a la legislación y las políticas relativas al acceso a la información del sector público](#), página 21 y siguientes.

¹⁴ Véase apartado 1 del artículo 6 b de la Directiva 95/46/EC.

¹⁵ Conviene señalar que algunos consideran que, dado que la reunión de distintos datos permite establecer perfiles personales, sería necesario prohibir la utilización comercial de los datos de carácter personal o por lo menos limitarla y sancionar las infracciones. Por lo que se refiere a los datos de carácter personal extraídos de fuentes oficiales, no hay ninguna excepción a la obligación de informar a la persona interesada (artículo 11 de la Directiva).

La Directiva 95/46/EC reconoce a la persona interesada el derecho a recibir información del tratamiento de los datos que le conciernen así como, cuando menos, el derecho a oponerse al tratamiento legítimo. Los ciudadanos deben pues ser informados de la finalidad de comercialización y poder oponerse a tal utilización mediante procedimientos simples y eficaces¹⁶.

En este aspecto, hay aún muchos progresos por hacer. La multiplicidad de fuentes de divulgación de datos, el gran número de agentes, la posibilidad de teledescarga, conducen a defender la idea de una ventanilla única de protección de datos que evite que los ciudadanos tengan de efectuar en multitud de ocasiones la misma diligencia ante el conjunto de los agentes. Eso es lo que ocurre, en varios Estados Miembros, con las listas telefónicas.

Es la razón también por la cual, el CNIL¹⁷ recomendó que todos los editores de listas telefónicas identifiquen para todos los soportes de publicación (papel, CD-ROM, Minitel o Internet) a los suscriptores que hayan ejercido su derecho a oponerse a la utilización de sus datos con fines comerciales.

Esta idea de ventanilla única parece esencial, tanto desde el punto de vista del respeto de los derechos de las personas, como desde el punto de vista de los agentes comerciales que deseen utilizar datos personales.

La conciliación del derecho a la intimidad y de los intereses comerciales de los agentes podría también conducir a que fueran necesarios el consentimiento de la persona¹⁸, o incluso medidas legislativas o reglamentarias, como puede ilustrarse con el siguiente ejemplo:

En un dictamen relativo a la comercialización de datos resultantes de licencias de construcción, la Comisión belga de protección de la intimidad consideró que una nueva finalidad (a saber, la comercialización de los tratamientos de las autoridades públicas), para ser lícita, debe estar legitimada por un fundamento legal o reglamentario que la defina de manera suficientemente precisa. A falta de tal legitimación, la Comisión considera que el interés que persigue la comunicación de los datos a terceros no prevalece sobre el derecho al respeto de la intimidad de la persona cuyos datos se comunican. Una tercera posibilidad consiste en la obtención del consentimiento del interesado para la finalidad de comercialización. Debe darse este consentimiento inequívocamente y con conocimiento de causa, habida cuenta del hecho de que quien desea obtener una licencia de construcción está obligado a presentar un expediente que responde a determinadas condiciones.

Más adelante, en el mismo dictamen, esta comisión belga describe la información de las personas, haciendo hincapié más concretamente en la existencia de un derecho de oposición, a requerimiento y de forma gratuita si los datos se hubieran obtenido con fines de comercialización directa.

¹⁶ Véase artículos 10, 11 y 14 de la Directiva 95/46/EC.

¹⁷ Comisión Nacional de Libertades e Informática, Francia.

¹⁸ Véase artículos 2 h), 7a y 8 de la Directiva 95/46/EC relativa a la definición de “consentimiento” así como la exigencia de formas específicas de consentimiento según el caso

CONCLUSIÓN:

El legislador, cuando desea que un dato se vuelva accesible al público no considera sin embargo que haya de convertirse en *res nullius*. Tal es la filosofía del conjunto de nuestras legislaciones. El carácter público de un dato de carácter personal, resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva, *ipso facto* y para siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana.

En el debate desarrollado en el marco de la consulta sobre el Libro Verde y en las conclusiones que de él se deriven, es conveniente tener en cuenta, sobre todo, los aspectos y cuestiones siguientes con el fin de reconciliar el respeto del derecho a la intimidad y a la protección de los datos personales de los ciudadanos con el derecho del público a acceder a la información del sector público:

- valoración caso por caso de la cuestión de si un dato de carácter personal puede publicarse / hacerse accesible o no, y en caso afirmativo, en qué condiciones y en qué soporte (digitalización o no, difusión en Internet o no, etc.),
- principios de finalidad y legitimidad,
- información de la persona en cuestión,
- derecho de oposición de la persona en cuestión,
- utilización de las nuevas tecnologías para contribuir al respeto del derecho a la intimidad.

Estas directrices parecen imponerse no solamente en las situaciones en las que existe una normativa relativa a la publicidad o el acceso, sino también en aquéllas en las que no parecen ser necesarias medidas reglamentarias para satisfacer la solicitud formulada por el público de acceder a información del sector público, incluidos los datos personales¹⁹.

Pendiente de las conclusiones de la Comisión Europea sobre la consulta en curso, el Grupo manifiesta ya desde ahora su gran interés en seguir contribuyendo a los trabajos previstos en este ámbito, así como en aquéllas cuestiones que se refieren a la puesta a disposición de terceros de las informaciones del sector público que sobrepasen el marco estricto del Libro Verde²⁰.

¹⁹ Véase nota de la página 2.

²⁰ Véase por ejemplo lo dicho acerca del apartado 56 (página 9 del Libro Verde) sobre la posibilidad de recogida y reparto de información así como el apartado 123 (página 19) referente a propuestas de actuación para el intercambio de información entre entidades del sector público.

Hecho en Bruselas, el 7 de mayo de
1999.

Por el Grupo

Peter HUSTINX

Presidente