Temas de Biblioteconomía

# Legislación española sobre protección de datos y su implicación en la gestión bibliotecaria

Autor: César Martín Gavilán

Fecha: 05/11/08

# Introducción

La utilización intensiva de la tecnología en la gestión bibliotecaria y documental incide de manera plena en el derecho de las personas a que sus datos personales sean tratados de forma rigurosa y segura. Y es que cuando hablamos de intimidad o protección de datos hablamos de control sobre *nuestra* información.

En la lista IWETEL se llevó a cabo durante 2005 y 2006 un debate sobre el tema de los ficheros de datos de préstamos de los usuarios de las bibliotecas (Asunto: Historial de préstamos). ¿Pueden guardarse los datos de los documentos prestados por un usuario? ¿puede éste negarse a facilitarnos alguno de sus datos personales? Es fácil encontrar en la ficción cinematográfica ejemplos de cómo las datos personales del uso de las bibliotecas se utilizan en investigaciones criminales. En *Todos los hombres del presidente* (1976), uno de los periodistas que está investigando el llamado Watergate llama ni más ni menos que a la Library of Congress para saber a qué libros ha accedido un congresista implicado en la trama. Dicha información se la facilitan ¡por teléfono! Otro ejemplo del celuloide lo encontramos en *Seven* (1995), película en la que los agentes responsables de la localización de un sociópata se hacen con los datos de préstamos de obras "satánicas" con el fin de localizar al criminal. Naturalmente, la realidad siempre supera a la ficción y los ficheros de préstamo de las bibliotecas y los listados de compras de las librerías se han convertido, Patriot USA Act mediante, en fuente de información de supuesta vital importancia en los EEUU para la investigación del terrorismo. Estos ejemplos poden de manifiesto la actualidad de la cuestión de la protección de los datos personales y la sensibilidad que despierta su recogida, tratamiento y difusión en las organizaciones.

¿Hasta qué punto una universidad puede hacer público el directorio de su personal en su web sin el permiso expreso de sus trabajadores? ¿Es lo mismo si estos datos de ofrecen solamente en la intranet? En la protección de datos personales hay que considerar en qué entorno se están haciendo accesibles datos considerados personales. Veremos posteriormente que, efectivamente, no es lo mismo ofrecer acceso a datos personales a usuarios de una intranet que al público en general a través de una web.

Se nos hace difícil imaginar una institución de cierta complejidad que no disponga de ficheros de datos personales. Las bibliotecas recogen datos de préstamo, de consulta de documentos especiales (tesis, etc.), de préstamo interbibliotecario, de adquisiciones, de personal, etc., pero la lista se hace casi infinita al considerar el resto de organizaciones. Si a esto añadimos el hecho de que en España tenemos una de las leyes más duras, en los que a sanciones se

refiere, deberemos extremar el celo al realizar las pertinentes auditorias a fin de garantizar el adecuado tratamiento de los datos personales que hayamos recogido. Frecuentemente, estos datos se hacen accesibles a través de las intranets de las organizaciones, por lo que será necesario disponer de los protocolos de trabajo adecuados para garantizar su licitud.

## Marco jurídico

Las tecnologías de la información y las comunicaciones han facilitado:

- la acumulación de grandes volúmenes de información personal aparentemente dispersa e inocua
- la extracción de información de carácter privado mediante técnicas de tratamiento que aprovechan elementos que en principio no poseen tal naturaleza

lo cual no deja de constituir un serio peligro que los legisladores no han pasado por alto.

Las diferentes legislaciones europeas se han ido adaptando al nuevo entorno tecnológico de la sociedad de la información modificando y ampliando sus respectivos marcos legislativos, en especial por la necesidad de incorporar al ordenamiento jurídico nacional las diferentes directivas comunitarias que el Parlamento Europeo ha ido aprobando hasta el momento.

El “derecho a la protección de datos”, de hecho, viene recogido en distintos textos internacionales, entre los que destacamos:

- Convenio del Consejo de Europa de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio 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 Constitución española (CE), además, no es ajena al fenómeno de la protección de datos personales. Al ser un texto “joven”, recogió en el momento de su promulgación los principios básicos a partir de los que se ha desplegado la legislación actual. Así, en su artículo 18.4 proclama que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el ejercicio pleno de sus derechos”.

Dicho precepto completa otros tres epígrafes del artículo 18 en los que se protege el derecho al honor, intimidad y derecho a la imagen (18.1), la

inviolabilidad del domicilio (18.2) y el secreto de las comunicaciones (18.3). Todos estos artículos forman parte del capítulo correspondiente a los llamados derechos fundamentales de la ciudadanía. De esta forma, tan "importante" es el derecho que tenemos a que nadie entre en nuestro domicilio sin el correspondiente permiso (excepto en los casos previstos por la ley) como el de la protección de nuestros datos personales. Al tratarse de un derecho fundamental, la ley de protección de datos tiene el rango de "ley orgánica", el mismo rango, por ejemplo, con el se aprueban los estatutos de autonomía (art. 81.1 CE).

En España, la legislación básica sobre protección de datos la encontramos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

Algunos aspectos de la legislación básica deben complementarse, además, con el reciente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Por otra parte, existe una sentencia del Tribunal Constitucional que anula algunos de los artículos de la LOPD (STC 292/2000, de 30 de noviembre de 2000), que resulta clave en nuestro marco jurídico para definir el *concepto de libertad informática* (Fundamento Jurídico 5), *distinguir entre libertad informática y derecho a la intimidad* (FJ 5), y establecer el *objeto y alcance del derecho fundamental a la protección de datos* (FJ 6).

Además, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia mediante sistemas de cámaras o videocámaras, puede ser de aplicación en el caso de que existan cámaras de vigilancia instaladas en los locales de una biblioteca.

Debemos tener muy presente que, aunque los datos personales sometidos a la LOPD se encuentren en ficheros de uso interno o en una intranet, el nivel de exigencia legal es el mismo que si fuera público. En no pocos casos, las denuncias por supuestos incumplimientos de la protección de datos se producen dentro de las organizaciones.

## Ley Orgánica 15/1999 (LOPD)

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) transpone la Directiva 95/46/CE al ordenamiento jurídico español y a las normas de aplicación, derogando y sustituyendo la primera ley de protección de datos conocida como LORTAD (Ley Orgánica

5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal), ley que no tuvo demasiada aceptación.

Objeto

Esta ley, según reza su art.1, tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

Ámbito de aplicación

En contra de lo que en principio pudiera parecer, esta ley no solamente es aplicable a los datos gestionados informáticamente, sino que también debe observarse para los personales recogidos y/o conservados exclusivamente en soporte papel. Así, el artículo 2.1. de la LOPD delimita su ámbito de aplicación a: "...los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". Como puede observarse se hace referencia a datos organizados almacenados en soporte físico; un listado en papel o una carpeta lo son.

La LOPD, de entrada, no determina expresamente qué datos debemos recoger y cuáles no, y mucho menos impide que se recojan datos personales en general. Así, por ejemplo, existe una cierta "leyenda urbana" que explica que no se pueden guardar los ficheros de datos de préstamos de los usuarios de las bibliotecas porque la ley lo impide. Formulado en estos términos podemos decir que dicha aseveración es incorrecta, puesto que la ley no impide a las bibliotecas recoger estos datos. Ahora bien, ya que efectivamente son datos personales, la ley sí marca qué, cómo y hasta cuándo podemos gestionarlos.

Definiciones

Paralelamente, la ley define en su art. 3 toda una serie de conceptos necesarios para su correcta aplicación, entre los que destacamos:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de

datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

A partir de estas definiciones podemos realizar las siguientes observaciones:

– Los datos protegidos tienen que hacer referencia a personas físicas. Dicho de otra forma, no se regirán por la LOPD los datos referidos exclusivamente a personas jurídicas. Es decir, la denominación social, razón social, teléfono, etc. concernientes a una empresa no está aparado por la LOPD.

– El concepto de fichero tiene un amplio alcance. Si en la anterior Ley 5/1992 de protección de datos, ahora derogada, se hacía especial mención a ficheros automatizados (art. 3.b), la vigente LOPD solamente se refiere a fichero como forma de organización de datos, pero sin limitarse al ámbito digital. Así pues, un listado en el que los usuarios de una biblioteca deben registrarse para poder acceder a un ordenador portátil también tendría la consideración de fichero de datos personales (dado que el usuario es una persona física).

– En la enumeración de los diferentes tratamientos a los que podemos someter los datos personales queda otra vez patente la no exclusividad del tratamiento informático. Es decir, el tratamiento podrá ser informático, o no, solamente se precisa que los datos puedan ser grabados (en papel por ejemplo) para considerar que ya los estamos manejando.

– Se introduce en la ley la necesaria existencia de un responsable de los ficheros (automatizados o no) que podrá ser una persona física o jurídica y que será la responsable del cumplimento de todos los requisitos que marca esta ley. Es importante que las organizaciones presenten cuántos ficheros susceptibles de incluir datos personales manejan su personal ya que serán ellas las responsables ante la ley.

– Cualquier puesta a disposición de terceros de datos personales es una "cesión o comunicación de datos". Con dicho concepto se definirá cualquier acceso que se realice por terceras personas a los ficheros de datos personales y que puede ser físico (consulta de un listado) o virtual (a través de la intranet, de un PC local, de una página, web, etc.). Debemos entender por cesión cualquier revelación que hagamos de datos personales independientemente del medio (de forma oral, escrita, entre ordenadores, etc.).

## Principios de la protección de datos

Al hablar de protección de datos cabe establecer un equilibrio entre la sociedad de la información y las libertades de los ciudadanos. Es obvio que las organizaciones necesitan datos personales para su normal funcionamiento. ¿Cómo sería posible, por ejemplo, realizar préstamos de documentos si no fuera posible registrar quién se lleva una obra?

De este modo, la LOPD establece una serie de principios para la recogida y gestión de datos personales cuya filosofía se podría resumir en el *mínimo de datos necesarios* y el *máximo posible de protección*. Podemos considerar que toda la legislación de protección de datos personales tiene como base el *principio de precaución*: es decir, las medidas señaladas en la ley intentan directamente prevenir un mal uso de los datos personales. Es desde esta perspectiva preventiva bajo la que se considera que es necesario trabajar.

Entre los principios que rigen la gestión de los datos personales, según la LOPD, podemos destacar:

- Calidad de los datos (art. 4).
- Derecho de información en su recogida (art. 5).
- Consentimiento del afectado (art. 6) y datos especialmente protegidos (art. 7).
- Seguridad de los datos (art. 9).
- Deber de secreto (art. 10).
- Comunicación de datos (art. 11).

<u>Principio de calidad de los datos</u>

Vendrá determinada por:

- La idoneidad de la información recogida.
- La veracidad.
- El tiempo de almacenamiento.
- La forma en cómo se recojan.

¿Qué datos podemos recoger? El artículo 4.1 de la LOPD estipula 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”.

El hecho de que los datos sean “adecuados”, término demasiado impreciso, pretende reducir al mínimo posible necesario los que se estén recogiendo. Los que solicitemos deben de ser lógicamente necesarios para el objetivo que nos hemos propuesto, y solamente para eso. Así por ejemplo, en un formulario que tengamos en nuestra web para que un usuario comunique una incidencia con el servicio de préstamo parece lógico solicitar el correo electrónico. Sería más difícil de considerar la obligación de hacerle facilitar su edad, puesto que el objetivo es la solución de una incidencia de circulación. Lo más sensato en estos casos es partir del principio que cuantos menos datos solicitemos mejor.

Otra cuestión a dilucidar es hasta qué punto podemos utilizar los datos recogidos inicialmente para una finalidad determinada, con el objetivo de usarlos para una función distinta. Sería el caso del fichero de datos personales de los usuarios de un servicio determinado: podrían ser utilizados para ofertar otro. Esta cuestión no es menor y generó una considerable polémica en el trámite de aprobación de la ley. El art. 4.2 determina 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”. Nótese que se utiliza el término “finalidades incompatibles” y no “finalidades distintas” con lo que el legislador quiso no restringir totalmente la reutilización de datos, asumiendo en todo caso, suponemos, el riesgo de la imprecisión de la definición. Pero, ¿qué debemos considerar por “finalidades incompatibles”?

Desde la óptica del principio de precaución al que nos referíamos al principio, se nos antoja que debemos ser estrictos en restringir al máximo la consideración de finalidades compatibles. Siguiendo con en el ejemplo que citábamos del préstamo a domicilio, los datos que fueron recogidos para esa función; solamente deberíamos considerarlos compatibles para ello, servicios exactamente similares o que substituyan, amplíen o mejoren esta actividad inicial. Imaginemos una biblioteca que dispone de los datos personales de lectores del servicio de préstamo y se plantea si pueden ser utilizados para remitir electrónicamente un boletín de nuevas adquisiciones. No sería adecuado utilizarlos automáticamente sin pedir la conformidad a los usuarios inscritos, puesto que la recogida de datos tenía exclusivamente como misión la utilización del servicio de préstamo. Sería mucho más adecuado remitirles un correo electrónico informándoles del nuevo servicio y de la posibilidad de autorizar la inclusión de sus datos para recibir el boletín de novedades, o mucho mejor, publicitar el nuevo servicio y que cada usuario decida si quiere activar o no el nuevo servicio. Distinto sería el caso de los “Avisos de cortesía”

que anuncia con antelación la próxima finalización de un préstamo. Al ser un servicio que mejora un servicio ya existente, el préstamo, resulta absolutamente legítimo reutilizar los datos existentes sin necesidad de solicitar permiso a los afectados.

Este mismo artículo nos aclara que los datos recogidos sí que pueden ser utilizados a efectos de estudios históricos, estadísticos o científicos. Aceptando, en todo caso, que se realizan por el mismo servicio que lo lleva a cabo.

¿Debemos actualizar los datos? Una función del responsable del fichero de datos personales es mantenerlo actualizado de forma que la información personal almacenada sea cierta. El art. 4.3 subraya que "los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado". Aparte del hecho que se supone que la organización es la primera interesada en mantener al día los registros de sus bases de datos, debemos recordar que los afectados tienen derecho a conocer qué informaciones tenemos sobre ellos y, en todo caso, exigirnos la rectificación de todo lo que no se corresponda con la realidad (art. 4.4).

¿Cuánto tiempo debemos guardar los datos? El período durante el que debemos conservar los ficheros de datos personales es una cuestión que deben tener muy en cuenta los responsables del sistema de información de la organización. Dicho aspecto queda relacionado, en términos documentales, a la gestión general de la documentación de las organizaciones. Es conocido que los sistemas archivísticos prevén unas tablas de conservación y eliminación de documentos que tienen como función gestionar el destino final de los materiales almacenados. En el momento de determinar los plazos de eliminación deberemos tener muy en cuenta la LOPD para conservarlos como mínimo, durante el tiempo que se deriva de la aplicación de la ley.

Este concepto es aplicable igualmente a los ficheros de datos personales de nuestra organización. A tenor de lo que expresa el art. 4.5 "los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".

El principio general será pues, que los datos personales solamente se guardarán mientras esté vigente la función para la que fueron recogidos. En caso contrario deberán ser cancelados (art. 16.3): "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".

Así pues debemos distinguir entre cancelación/bloqueo de los datos y eliminación definitiva del registro. En el primer caso se impide la utilización de dicha información para el uso que habíamos previsto, mientras que la eliminación incluye su destrucción física.

A efectos de la correcta gestión de la protección de datos personales, el sistema de gestión documental de la organización deberá determinar en qué momento podemos eliminar físicamente los datos de un fichero en concreto. La LOPD no marca un plazo determinado: "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" (art. 16.5). Debemos entender por "disposiciones aplicables" la legislación que regula los períodos de conservación de la documentación en general, incluida, la misma LOPD. A falta de un plazo concreto, intentaremos calcular el tiempo mínimo y máximo durante el cual podemos (o debemos) conservar los ficheros de datos personales no utilizados:

– Mínimo. Decíamos que la LOPD no fija un plazo concreto a partir del que podamos eliminar efectivamente cualquier tipo de dato. Esto es debido al hecho de que ya existe o podría legislarse en el futuro un plazo de conservación específico en función del tipo de dato (por ejemplo, los relativos a la salud). A pesar de ello podemos fijar en tres años el período mínimo de conservación de cualquier tipo de datos personal. El cómputo es el resultado de observar el artículo 47 de la misma ley referente a la prescripción de las posibles infracciones; aquellas de carácter leve prescriben al año, las graves a los dos, mientras que las muy graves lo hacen a los tres. En todos los casos a partir de la fecha de la comisión de la presunta infracción. Dicho de otra forma, durante un plazo máximo de tres años a partir de su creación, modificación u otro proceso (en el cupiera infringir la legislación) nos podríamos encontrar con la apertura de un procedimiento de infracción por lo que es aconsejable conservar los datos como mínimo durante ese período.

– Máximo. No viene marcado en la LOPD, solamente se prescribe 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. 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." (art. 4.5). Así pues no parece que una conservación indefinida sin justificación sea adecuada a tenor de este artículo. Deberemos en cada caso decidir durante cuánto como máximo conservaremos los datos personales que ya no se utilizan. Por ejemplo, es legítimo conservar los datos de un antiguo usuario mientras tenga préstamos pendientes y la biblioteca no renuncie a

su derecho de reposición o al reintegro del valor del material perdido, a pesar de que la función para la que fueron recogidos los datos esté caducada.

Debemos insistir nuevamente en la necesidad de estudiar si los datos personales que almacenamos se encuentran regulados por alguna normativa específica diferente de la LOPD, ya que en este caso el tiempo mínimo de conservación podría ser superior (historias clínicas, datos contables con datos personales, expedientes administrativos, etc.).

Principio de información en la recogida de los datos

El responsable del fichero tiene el deber de informar a la persona afectada del hecho que sus datos serán recogidos en un fichero. Esta obligación es una de las bases que permiten ejercer de forma efectiva los derechos de los afectados. Estas informaciones, que deben aparecer en los formularios de recogida de información, se regulan a través del art. 5 de la LOPD y serán comunicados de forma expresa, precisa e inequívoca (art. 5.1):

- 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.

- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Cabe señalar que la recogida de datos no será lícita si no se cumplen las condiciones de este artículo. Se prevén, igualmente una serie de excepciones a la norma general en los casos de que el objetivo de la recogida haga obvia la justificación del dato (art. 5.3) o los datos no hayan sido facilitados por el propio afectado (art. 5.4 y 5.5).

Principio del consentimiento informado

La norma general es clara. Cualquier tratamiento de los datos personales debe de contar con el consentimiento expreso del afectado: “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa” (art. 6.1). Como se define en el art. 3.h. de la LOPD, entenderemos por “consentimiento del interesado” “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.

Esta norma general es lo que posibilita la llamada *autodeterminación informativa de la ciudadanía*: es el ciudadano quien tiene el control de sus datos.

Así pues, en los textos informativos anexos a los formularios de recogida de datos personales (en papel o web) deberemos añadir una mención expresa conforme se autoriza a la organización al tratamiento de los datos. La ley prevé igualmente una serie de excepciones en lo que respecta al consentimiento informado. No será necesario cuando: “los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación mercantil, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del art. 7.6 de la LOPD, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado” (art. 6.2).

Datos especialmente protegidos

En consonancia con el art. 16.2 de la Constitución, la LOPD enumera una serie de tipos de datos que son especialmente sensibles y sobre los que no se puede obligar a nadie a facilitarlos. Se entenderá por datos especialmente protegidos aquellos que hagan referencia a la ideología, la afiliación sindical, la religión o creencias, el origen racial, la salud y la vida sexual de las personas. No todos ellos tienen el mismo nivel de legislación ya que la LOPD viene a establecer datos especialmente protegidos de primer y segundo grado. Alguno autores llegan a hablar de hasta tres tipos.

Muchos profesionales de la información pueden llegar a gestionar en sus ficheros datos personales que podrían asimilarse a alguna de estas categorías: es el caso de los expedientes de bajas laborales por enfermedades, incapacidades temporales o permanentes, afiliación sindical, etc.

Igualmente, algunos centros documentales como bibliotecas, archivos o centros de documentación podrían querer ofrecer servicios a grupos concretos de usuarios con necesidades específicas como inmigrantes, personas con movilidad reducida, problemas de visión, colectivos religiosos concretos, etc. Para hacer llegar estos servicios sería necesario recabar datos especialmente protegidos, por lo que en todo caso es conveniente primero realizar un estudio de las características de los mismos y las condiciones bajo las cuales dicha información puede ser tratada. Por ejemplo, el préstamo especial (facilidades, condiciones mejoradas, plazos ampliados) para minusválidos en una biblioteca obliga a gestionar datos especialmente protegidos.

Principio de la seguridad de los datos

Una vez que se han cumplido con todos los requisitos necesarios para recopilar y tratar datos personales, el responsable del fichero tiene la obligación de garantizar su seguridad. En este sentido, la LOPD obliga a aplicar una serie de medidas tendentes a garantizar que nadie podrá acceder a los datos personales que tenemos custodiados a no ser que sea en cumplimiento de lo marca la ley (art. 9.1). Es más, se impide expresamente disponer de datos personales si no somos capaces de garantizar los niveles de seguridad exigidos (art. 9.2).

Recientemente hemos podido asistir a la polémica generada por el hecho que la Dirección General de Tráfico permitía el acceso a los conductores a sus expedientes personales para consultar el saldo de los puntos de su carnet de conducir. Al parecer las medidas de seguridad previstas (DNI y fecha de expedición del mismo) resultaban insuficientes al no exigirse además una clave personalizada. Un acceso poco seguro al área personal “Mi cuenta” de un OPAC de biblioteca, donde es posible consultar datos personales, ver los préstamos en curso, sanciones, realizar reservas, etc. podría generar una polémica similar.

La normativa que regula las condiciones de seguridad a aplicar en ficheros de datos personales se encuentra en el reciente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Los requerimientos de seguridad del Real Decreto 1720/2007 se basan en la definición de tres niveles de seguridad (bajo, medio y alto). Cada uno conlleva la aplicación de una serie de medidas concretas como pueden ser la elaboración de un protocolo de seguridad, la creación de un registro de incidencias, control de los accesos (virtuales o físicos, etc.). En función del tipo de datos personales que contenga el fichero deberemos ir acumulando las medidas de protección que se apliquen. Así, todos los ficheros con datos personales deberán cumplir las medidas de seguridad del nivel básico. Si los

datos personales son relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, etc (art. 81.2. RD 1720/2007), a las medidas de seguridad del nivel básico deberemos sumar las del nivel medio. Finalmente, en el caso de los datos personales especialmente protegidos deberemos también sumar las medidas de seguridad del nivel alto.

¿Cómo se consiguen los objetivos de la seguridad informática (confidencialidad, integridad y disponibilidad) de las bases de datos? Esencialmente mediante medidas organizativas y técnicas. Entre las medidas organizativas destaca la definición de una política de seguridad, la definición de funciones y responsabilidades de los usuarios de los datos, la articulación de los procedimientos a seguir (en la recogida de datos; en el acceso, rectificación y cancelación de los datos; en la notificación de incidencias), el registro de cualquier incidencia, la formación continua de los usuarios de los datos, los controles periódicos del cumplimiento de la política de seguridad, la gestión de los soportes de los datos, las explotaciones del fichero, etc.

El deber de secreto

Esta ley exige a quienes intervengan en cualquier fase del tratamiento de los datos a guardar secreto profesional sobre los datos, manteniéndose la obligación incluso después de finalizar su relación con el responsable del fichero. La obligación de confidencialidad no es nueva ni exclusiva de esta ley; se trata de un deber moral ampliamente recogido en otra legislación. Constituye la adaptación al ámbito informático del deber de reserva o sigilo, y está relacionado con el deber de secreto profesional. Faltar al deber de secreto se configura como infracción leve (art. 44.2.e) grave (44.3 g) o muy grave (44.4.g), dependiendo del tipo de infracción. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca las normas de seguridad así como las consecuencias en que pudiera incurrir en caso de incumplimiento del deber de secreto.

Comunicación de datos personales

Recordemos que por comunicación (o cesión) de datos personales entenderemos: “toda revelación de datos realizada a una persona distinta del interesado” (art. 3.i LOPD). Así pues, entra dentro de esta categoría permitir el acceso en cualquier forma (personalmente, por teléfono, por escrito, a través de intranet, etc.) a otras personas que no sean el usuario.

En el entorno de un SIGB es frecuente dar acceso a los miembros de la biblioteca a ficheros que pueden contener datos personales (registros de usuario, registros de autoridad, registros de proveedores autónomos, etc.). ¿Estamos en este caso también haciendo una comunicación de datos? ¿podemos dar acceso universal a ficheros con datos personales a todos los miembros de la organización? De manera general no. Recordemos que el

principio de calidad de recogida de datos personales (art. 4.1) restringía el tratamiento al "ámbito y finalidades determinadas". Así pues, solamente aquellas personas relacionadas directamente con la función concreta para la que se han recogido los datos podrán acceder a ellos. Podríamos ejemplificarlo con el supuesto ya comentado del fichero de préstamos de obras. Entendemos que solamente las personas asignadas circulación deberían poder acceder a esa información ya que les es necesaria para el desarrollo de sus funciones.

Aclarado este punto, como principio general deberemos observar que ninguna comunicación o cesión de datos personales está autorizada sin previo consentimiento del afectado (art. 11.1) a excepción de los supuestos contemplados en el art. 11.2, entre los que destacamos que así lo marque una ley, sean datos de fuentes accesibles al público (definidas en el art. 3.j) o cuando dicha comunicación sea necesaria para el ejercicio de una relación jurídica aceptada previamente (cuando realizamos un pedido y el proveedor facilita al transportista externo nuestros datos personales para la entrega de la mercancía).

Igualmente deberemos analizar si la comunicación de datos personales de índole laboral a través del web cumple con las normas previstas (un ejemplo sería el de los directorios de empresas e instituciones). Nadie duda de la utilidad que reporta a un usuario poder localizar a través del directorio institucional al responsable de un determinado servicio. Ahora bien, teniendo en cuenta que un directorio de personal se identifica a una persona, estamos delante de una comunicación de datos de carácter personal. A todos los efectos, la dirección de correo electrónico (aunque tenga formato institucional, por ejemplo "@ucm.es") se considera dato personal. El principio general es claro: debemos contar con la autorización de la persona en cuestión para hacer público su nombre y dirección de correo electrónico. Otra cosa muy distinta sería que dicha información se facilitara en un entorno limitado (por ejemplo, una intranet sólo accesible para personal y usuarios del servicio realizado por esa persona).

## Registro de ficheros

De manera sucinta solamente haremos referencia a la necesidad de registrar cualquier fichero que contenga datos personales. Los ficheros de titularidad privada (empresas, etc.) deben hacerlo a través de la Agencia Española de Protección de Datos, mientras que las administraciones públicas podrán hacerlo en esta misma agencia o a través de las agencias de protección de datos autonómicas existentes (es el caso de la Comunidad de Madrid, Euskadi y Catalunya). En cuanto a los ficheros de titularidad pública, igualmente deberá

publicitarse su existencia a través del BOE o diario oficial autonómico correspondiente.

A modo de ejemplo, la UV tiene en estos momentos dos ficheros registrados vinculados con el SBD: “Usuarios bibliotecas UVEG”, cuya finalidad es la gestión administrativa del préstamo de material bibliográfico de las bibliotecas de la Universitat de Valencia, y “Usuarios préstamo interbibliotecario”, cuya finalidad es la gestión administrativa del préstamo interbibliotecario de la UVEG (resolución del rectorado de 10 de julio de 2001).

## Procedimientos derivados de la aplicación de la LOPD

La LOPD reconoce una serie de derechos a los titulares de los datos personales (Título III), que en su aplicación generan determinados procedimientos, entre los que podemos destacar:

Derecho de oposición: En la mayor parte de los casos el tratamiento de datos por parte de la Administración no requiere el consentimiento del titular de estos (art. 6.2). A pesar de ello, para este tipo de supuestos se establece el derecho del afectado a oponerse a los tratamientos, excepto cuando la ley disponga otra cosa, “cuando haya motivos fundados y legítimos relativos a una situación personal concreta” (por ejemplo, acoso sexual dentro de la organización). En estos supuestos, el responsable del fichero excluirá del tratamiento los datos referidos al afectado.

Derechos de acceso, rectificación y cancelación: El ejercicio del derecho de acceso no supone necesariamente los de rectificación o cancelación de los datos, puesto que son derechos que se ejercen de una manera independiente aunque, entre las causas que podrían legitimar el acceso se encuentra, obviamente, la verificación de la corrección o existencia de los datos con motivo de una rectificación o cancelación posterior.

*Derecho de acceso* (art. 15): El interesado tiene derecho a solicitar y a 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”.

*Derecho de rectificación y cancelación* (art. 16): Se trata de corregir o eliminar los datos que sean inexactos o incompletos, inadecuados o excesivos. La rectificación podrá realizarse a instancia de la parte interesada. No obstante, cuando el gestor de un fichero detecte un error lo corregirá si conoce el dato correcto o solicitará la información correspondiente para enmendarlo. Asimismo, cuando se constate que no

había ningún motivo para tratar un dato o cuando haya cesado la finalidad para el cual se había pedido, se cancelará.

# Conclusiones

La protección de datos es una parte del complejo mundo jurídico que la automatización de la gestión de la información ha situado en el primer plano de la actualidad profesional. Los principios que rigen la protección de datos personales pretenden preservar la intimidad de todos nosotros y nos permite tener el control total sobre nuestros datos más íntimos. La ley marca un camino a seguir para poder gestionar los datos que necesitemos de nuestros usuarios con el fin de hacer compatible el derecho de unos a su intimidad y la necesidad de las organizaciones a disponer de los datos necesarios para ejercer sus finalidades.

## BIBLIOGRAFÍA

Vives-Gràcia, Josep: "Confidencialidad y derechos de autor en un proyecto de intranet". En: *El profesional de la información*, v.16, n. 3, mayo-junio 2007.

Martínez Martínez, Ricard: “Protección de datos de carácter personal en la UVEG”. Presentación ppt (14/6/2004)
http://biblioteca.uv.es/intranet/mil/personal/proteccio_dades.pdf

http://www.uv.es/siuv/cas/normativa/proteccio.wiki