Panorama de la Legislación Europea sobre Protección de Datos Personales

STEWART H. DRESNER
Licenciado en Ciencias Políticas y Marketing.
Universidad de Lancaster (Reino Unido).
Director de Privacy Laws & Business.
(Traducido por SANTIAGO RIPOLL CARULLA)

Introducción.

1. El pasado 15 de enero, en Madrid, tres personas fueron arrestadas por la policía acusadas de estar involucradas en la venta de datos personales procedentes del Centro de Informática del Departamento de Trabajo y de Seguridad Social.

El banco de datos del que disponían contenía información de más de 2 millones de ciudadanos españoles, y hacía referencia, entre otros, a los siguientes aspectos: D.N.I., sexo, estado civil, nombre y dirección, datos familiares (por ejemplo, número, edad y sexo de los hijos), nivel de ingresos, información sobre la vivienda y otros gastos, etc.

En mi intervención trataré de exponer el modo en que una actividad de este tipo estaría regulada por las leyes de protección de datos en la mayoría

del resto de paises europeos, así como la importancia de los principios contenidos en la Convención del Consejo de Europa sobre protección de datos.

Por supuesto que, dado que este escándalo ha producido un considerable impacto en la opinión pública española, es posible deducir de él algunas consecuencias positivas:

-Se ha adquirido conciencia de la necesidad de poseer una efectiva regulación de los datos personales;

-Ha permitido advertir la conveniencia de ampliar a través de una ley el contenido de la protección dispensada en esta materia por el artículo 18 de la Constitución española;

-Ha concienciado al Gobierno y al Parlamento de la importancia de contar con una adecuada legislación en materia de protección de datos, provocando una agilización en sus tareas al respecto.

2. Obviamente, en países que ya contaban con legislación sobre protección de datos ha habido también escándalos similares al ocurrido en España. Así, el asunto Burberrys, acaecido en Francia. Burberrys, la firma británica de confección de prendas de ropa de alta calidad, creó un banco de datos de sus clientes con el objetivo de informarles puntualmente sobre sus nuevos productos.

Cuando estas listas fueron empleadas por un candidato de extrema derecha en unas elecciones municipales para formalizar un mailing sobre su candidatura, fueron decomisadas por la Autoridad Francesa de Protección de Datos (Comission National Informatique et Libertés, CNIL) por no haber sido empleadas con la finalidad para la que se recopilaron inicialmente.

En buena lógica, no fue suficiente defensa para Burberrys el argumentar que el perfil de sus clientes (varones de elevada posición social) emparejaba bien en principio con los potenciales votantes del partido en cuestión.

La ley de protección de datos francesa contiene un principio esencial, el deber de informar al momento de la colecta de los datos de la finalidad para la que se emplearan.

3. Este episodio, pues, sirve para ejemplificar como el derecho de la protección de datos desplaza el punto de equilibrio desde la industria y los gobiernos a aquellos individuos cuyos datos son recolectados, almacenados y

procesados. Esta nueva situación resulta cuando menos incómoda para las empresas y las autoridades gubernamentales, acostumbradas a contar con altísimos niveles y con poderosos mecanismos de obtención de información relativa a sus ciudadanos y clientes en aras - se argumenta - de una mayor eficacia en su gestión.

Sin embargo, conviene mirar más allá de estas incomodidades inmediatas y proteger, así, la dignidad del individuo.

I. Las leyes europeas de protección de datos.

4. En el cuadro número 1 se recoge de forma gráfica el panorama de las leyes europeas de protección de datos. Por el momento, no nos detendremos en un examen profundo de este cuadro. Es suficiente con advertir que, aunque existen algunos principios comunes a estas leyes, también hay diferencias entre ellas.

Idéntico ejercicio debe realizarse en relación al cuadro número 2, donde el lector encontrará la totalidad de los proyectos de ley existentes actualmente en Europa.

Consideremos esta información desde una nueva perspectiva: los cuadros 3 y 4 reflejan los países europeos que cuentan ya con ley de protección de datos o bien que han elaborado un proyecto de ley sobre la materia, respectivamente.

En relación a los primeros, cabe indicar que Suecia fue el primer Estado en elaborar una normativa sobre la materia (1973), mientras que Holanda (1988) y Portugal (1991) han sido los últimos en hacerlo. Por otra parte, puede avanzarse que a finales de 1992 Bélgica, España e Italia verán aprobados sus respectivos proyectos de ley, de modo que el próximo año prácticamente todos los miembros de la Comunidad Europea (excepción hecha de Grecia) tendrán legislación sobre el tema. Esta normativa, por lo demás, se verá complementada con una Directiva comunitaria, cuyos postulados obligarán a cualquier organización que recopile y procese datos personales en un país miembro.

Procedamos a un examen algo más detallado de las diferentes leyes europeas de protección de datos personales.

5. En primer lugar, cabe indicar que su principal punto en común es el que todas ellas regulan el tratamiento de los datos automatizados o procesa-

dos, sin detenerse, pese a ello, en consideraciones sobre las características del proceso de informatización.

Todas las leyes:

-protegen a los individuos, entendiendo por éstos tanto a las personas físicas como a las jurídicas,

-reconocen el derecho de acceso y rectificación,

-establecen un sistema de recursos, de forma que si un individuo ve dañados sus intereses cuenta con mecanismos para obtener una compensación. A diferencia de la legislación estadounidense, las leyes europeas recogen la figura de la Autoridad de Protección de Datos, que hace las veces de ombudsman en la materia. Asimismo, los tribunales nacionales están capacitados para sancionar a las organizaciones públicas o a las compañías privadas que vulneren la ley.

6. La Convención del Consejo de Europa sobre protección de datos establece los principios que han de caracterizar a las legislaciones europeas. Éstos son susceptibles de ordenarse en tres grupos:

Derechos de los individuos:

-el derecho a conocer la existencia de un fichero que contenga información sobre uno mismo,

-el derecho de acceso a tal fichero;

-el derecho a exigir la corrección de los datos erróneos.

2. Responsabilidades de los titulares del fichero:

-recolección imparcial y legal de los datos,

-garantía de que la recopilación y el almacenamiento de los datos se realiza con una finalidad legítima y concreta, y que la información no es empleada con fines ajenos a los especificados,

-adecuación entre los objetivos a alcanzar con la configuración del banco de datos y el número y la calidad de los datos recopilados,

-exactitud de los datos y, cuando sea necesario, puesta al día de los mismos,

-obligación de destruir los datos personales contenidos en el fichero cuando ya no resulte necesario su almacenamiento.

3. Deberes de los usuarios:

-el responsable del fichero debe ser fácilmente identificable, lo que en la práctica se traduce en que sea conocido por el personal de recepción o por los miembros de la asesoría jurídica de la empresa,

-el acceso a los ficheros por parte de los individuos afectados no debe ser oneroso. En muchos Estados, la normativa impone la obligación de abonar a la empresa una cuota por disco consultado. Esta cuantía únicamente será devuelta en el supuesto de que el individuo advierta un error en la información,

-cualquier corrección que se realice deberá notificarse a la fuente de la que se obtuvieron los datos, para evitar así que se perpetúen los errores,

-instauración de un régimen de recursos y sanciones, que se entiende esencial para corregir posibles injusticias.

7. Junto a estos elementos comunes, las leyes europeas presentan también ciertas diferencias. En nuestra exposición nos referiremos tan sólo a algunas de ellas. Así, las legislaciones de algunos Estados atienden no sólo las bases de datos automatizadas, sino también los ficheros manuales, ya que se entiende que la garantía de los principios indicados no depende solamente de los mecanismos de recopilación y ordenación de los datos.

En cualquier caso, incluso en este grupo de leyes, los requisitos que se exigen de cara al registro de los datos únicamente se predican de los ficheros automatizados, nunca se hacen exigibles a los bancos de datos manuales.

Quizás, aquellos de Uds. que estén más familiarizados con el tema se hayan sorprendido de que no me haya referido hasta este momento al tema del registro. La razón es que este enfoque - que ciertamente ha sido el más usual mientras los objetivos perseguidos por las diferentes leyes era ordenar los procedimientos de recopilación masiva de información - resulta en la actualidad algo desfasado. Con todo, dado que la mayoría de las leyes europeas sobre protección de datos actualmente en vigor se basan en este modelo, expondré brevemente las características de lo que podemos

denominar el modelo sueco, inspirador de la primera generación de leyes sobre la cuestión.

II. El modelo sueco.

8. Suecia fue el primer Estado en contar con una normativa que cubriera a la vez los bancos de datos del sector público y del sector privado. Para comprender esta opción recordemos el contexto en que se aprobó la ley sueca en 1973.

En tal fecha, el principal problema estribaba en el hecho de que los datos personales se almacenaban en grandes ordenadores centrales, de modo que resultaba muy difícil determinar la presencia de una información. Incluso cuando se conocía que esta información además de almacenada había sido ordenada de un modo u otro - configurándose así, por ejemplo, ficheros policiales o de carácter fiscal, en el sector público, o bancos de datos relativos a la situación laboral de los empleados de una empresa o a la situación crediticia de los clientes de un banco, en el sector privado -, resultaba imposible acceder a ella. Lo que es peor ni tan siquiera existían mecanismos que garantizaran a los individuos afectados el derecho a acceder a esta información. Paralelamente, las empresas y organismos públicos se consideraban titulares exclusivos, propietarios de los ficheros así estructurados, de suerte que consideraban que un acceso a ellos resultaba un menoscabo a sus derechos de propiedad.

El modelo sueco de un sistema de registro masivo fue diseñado precisamente para dar nuevos derechos a los particulares afectados, y para imponer nuevas responsabilidades a las organizaciones del sector, fueran éstas públicas o privadas. En definitiva, se trataba de asegurar:

-un registro central de todos los bancos de datos del país;

-la Autoridad de Protección de Datos es la única con potestad para permitir a los responsables de los bancos de datos existentes el configurar ficheros a partir de determinados datos (raza, religión, conductas sexuales...), que se consideraran sensibles;

-los particulares tienen derecho a informarse sobre los datos que cada organización posee sobre ellos;

-los particulares tienen derecho a comprobar si una organización ha creado un fichero sobre ellos;

-los particulares tienen derecho de acceso a los ficheros relativos a su persona;

-los particulares tienen derecho a exigir la rectificación de la información errónea, o cuando menos a incluir en el disco su versión.

Junto a estos derechos y obligaciones, la Autoridad de Protección de Datos posee ciertos poderes que vienen sugeridos por su propia denominación, Datainspektionen, u Oficina de Inspección de Datos. Así, tiene capacidad para visitar los locales de las empresas del sector, incluso sin previo aviso, y para formalizar una inspección de los sistemas de seguridad del software, de la formación del personal,... Estas visitas de inspección pueden llevarse a cabo bien a instancias de la Oficina de Inspección, bien a raíz de una reclamación.

9. Este modelo tuvo una gran influencia y a semejanza suya fueron adoptadas las leyes de protección de datos adoptadas durante el año 1978 - Francia, Dinamarca, Noruega y Austria -, así como la legislación vigente desde 1979 en Luxemburgo, las normas adoptadas en Israel e Islandia en 1981, en el Reino Unido (1984), la Isla de Man y Guernsey (1986), y en Jersey (1987).

Desde hace unos diez años, pues, ha quedado establecido el modelo de legislación en la materia. Desde entonces la principal cuestión radicaba en averiguar cuál sería la próxima normativa aprobada y qué ligeras variaciones presentaría. La ley de protección de datos alemana, de 1977, resultaba ser la única excepción a esta situación, pues los mecanismos de garantía de la aplicación de los principios indicados eran ciertamente novedosos.

III. El modelo alemán de auto-regulación.

10. Mientras que hasta 1984, la ley alemana era el único elemento diferenciador en el panorama europeo de leyes sobre protección de datos, en la actualidad muchas de sus características están presentes en lo que podría denominarse la segunda generación de leyes sobre la materia.

Conviene, por lo tanto, detenernos brevemente en el estudio de la ley alemana para analizar después su influencia parcial en las leyes aprobadas en Finlandia, Irlanda y más recientemente en Holanda.

11. El aspecto principal de la ley alemana es el permitir el procesamiento de datos personales si el derecho lo permite o si el particular ha dado su consentimiento. A diferencia, por lo tanto, de lo que ocurre en otros países donde,

como hemos visto, el tratamiento de los datos únicamente resulta legal cuando se realiza bajo la supervisión de una autoridad central. Paralelamente, en la legislación alemana:

-el sujeto afectado debe estar informado del contenido de un fichero en el que por primera vez se haya almacenado información relativa a el mismo,

-se le concede el derecho de acceso previo pago de una cantidad que no debe exceder los costes directamente atribuibles al suministro de la información,

-los datos erróneos deben ser corregidos,

-es obligatoria la cancelación de los datos inexactos, así como de aquellos que ya no serán utilizados para el objetivo inicialmente previsto,

-los datos personales deben quedar protegidos por adecuadas medidas de seguridad.

12. A la vista de lo expuesto, cabe preguntarse porqué la ley alemana debe entenderse como un sistema de auto-regulación. Básicamente, por la inexistencia de un registro central.

A ello hay que añadir la exigencia de que cualquier compañía que configure un banco de datos de cierta importancia debe designar un Controlador de Datos de la propia compañía. Éste, que actuará como un órgano independiente, puede ser tanto un empleado de la compañía como un consultor o un abogado ajeno a la misma. En cualquier caso, no se le exige que se dedique en exclusiva a esta actividad. La única limitación que impone la ley es que su figura no llegue a plantear conflictos de intereses en la empresa, de modo que, por ejemplo, no podrá desempeñar esta función el Jefe de ventas de un empresa de marketing directo.

IV. Las razones de la actual prevalencia del modelo alemán.

13. Desde mi punto de vista tres razones permiten explicar el progresivo acercamiento durante los últimos años al modelo alemán.

a) *El rápido crecimiento de los micro-ordenadores*

14. Tal y como ha sido señalado previamente, el hecho que determinó la aparición de las primeras leyes de protección de datos fue el peligro de un almacenamiento anómalo de datos en grandes ordenadores centrales. De hecho, se entendía que una máquina que costaba millones de pesetas únicamente podría estar en posesión, y por tanto, ser utilizada por un número reducido de empresas. De ahí que el establecimiento de un sistema de registro centralizado resultara una medida idónea, incluso cuando empresas de tipo medio empezaron a trabajar con ordenadores.

Sin embargo, la proliferación de los micro-ordenadores durante los años 80 ha determinado que prácticamente todas las empresas, e incluso los particulares, puedan configurar su propio banco de datos, de modo que la eficacia de las legislaciones que fundamentan la protección de la intimidad en torno a un registro centralizado ha quedado mermada sensiblemente.

b) *Límites prácticos a la aplicación de la normativa inspirada en el modelo sueco*

15. En la actualidad nadie duda de la validez de los principios establecidos por las Directrices de la OCDE y por la Convención del Consejo de Europa. Con todo, la situación recién descrita ha planteado una importante cuestión, de carácter práctico. ¿Cómo puede la autoridad nacional de protección de datos percatarse de la existencia de pequeñas bases de datos, capaces, de infringir los principios reconocidos internacionalmente?

Supongamos una administración de fincas que elabora un listado de arrendatarios morosos, o un ambulatorio que confecciona una relación de pacientes adictos al alcohol, o una asociación patronal que recoge los nombres de los principales activistas sindicales del sector. Supongamos asimismo que estas pequeñas empresas ponen a la venta sus listados o, incluso, que ellas mismas los utilizan para impedir, vg., la contratación entre las sociedades agrupadas en la asociación patronal de los activistas incluidos en la lista.

En tales casos, las autoridades nacionales de protección de datos presentes en las leyes de protección de datos inspiradas en el modelo sueco únicamente podrán intervenir una vez hayan recibido la queja por parte del particular, esto es, cuando éste se haya visto ya directamente perjudicado.

c) *El movimiento internacional de datos*

16. Las tendencias en la regulación del movimiento internacional de datos han variado sustancialmente desde la adopción de la Ley sueca de protección de datos. En un principio, se consideraba que los datos objeto de

exportación debían ser férreamente controlados, entre otras cosas, porque el procesamiento de datos personales fuera de las fronteras nacionales podría llegar a minar el nivel de protección ofrecido por la ley interna.

Las autoridades de protección de datos de Suecia, Noruega y Austria han tratado por todos los medios de limitar los potenciales daños que podría causar a sus nacionales la exportación de algunos de sus datos personales. En general, los criterios para decidir la permisión o la prohibición de la exportación de los datos eran los siguientes:

-¿Cuál es el país de recepción de los datos? ¿Ha firmado y ratificado la Convención del Consejo de Europa?

-¿Cuál es la organización destinataria y cuáles son sus sistemas de seguridad, por ejemplo?

-¿Qué nivel de sensibilidad presentan los datos a exportar?

17. Por otra parte, las diferentes legislaciones nacionales han establecido diversas soluciones al respecto. De una parte, encontramos el "sistema de licencia formal" a toda exportación de datos, recogido por Suecia y Austria. De otra, el "sistema de notificación", característico de la legislación noruega, por el que se obliga a informar a la Autoridad de Protección de los datos de toda actividad de exportación. El sistema más flexible es el presente en las leyes francesa y británica, consistente en el deber de notificar la voluntad de exportar los datos a través de un formulario en el que se recogen otras cuestiones. Finalmente, la ley alemana carece incluso de mecanismos de control en este sentido, lo que no obsta a que los principios que informan la ley continuen vigentes, de forma que los particulares afectados mantienen sus derechos de acceso y de corrección incluso cuando sus datos estén recogidos en ficheros ubicados en el exterior.

Por lo demás, la práctica noruega de prohibir toda exportación de datos relacionados con información crediticia, ha abierto una nueva orientación destinada a proteger con mayor rigor los datos más sensibles. A veces, se ha tratado de solventar esta cuestión mediante la supresión de determinada información (el nombre, por ejemplo). Esta práctica, que se ha revelado útil respecto de determinadas actividades - la investigación médica, vg. - es, sin embargo, enormemente perjudicial para el sector del marketing directo.

Por último, conviene señalar que la prohibición presente en la ley sueca de exportar a un país que no sea parte en el Convenio del Consejo de Europa

cualquier tipo de datos personales cede si el particular afectado da su consentimiento. La cuestión del consentimiento, pues, resulta capital, por cuanto puede dar a las empresas de marketing directo o a las sociedades bancarias la llave para proceder a una exportación que, en principio, dada la naturaleza de los datos o el país de recepción, era ilegal.