IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

Perspectivas del derecho a la autodeterminación informativa

Pablo Lucas Murillo de la Cueva

Fecha de presentación: mayo 2007
Fecha de aceptación: junio 2007
Fecha de publicación: septiembre 2007

Resumen

La situación en que se halla el ordenamiento jurídico español en materia de protección de datos es en cierto modo contradictoria, ya que existe un reconocimiento del carácter fundamental del derecho a la protección de datos y un marco jurídico que lo desarrolla, sin embargo, las regulaciones sectoriales de este derecho son insuficientes.

En el ámbito público, existe una normativa que tiene implicaciones directas con el tratamiento de datos de carácter personal (DCP), alguna en fase de aprobación, que en ocasiones únicamente se remiten a la LOPD, y en otras es un tanto contradictoria con dicha ley orgánica. En cualquier caso, la AEPD y los tribunales deberán ser especialmente exigentes en su aplicación, a fin de proteger no sólo el derecho a la autodeterminación informativa, sino más allá, la propia libertad de las personas.

El sector privado requiere de una mayor atención, ya que no se halla sujeto a condicionamientos institucionales y los DCP constituyen un bien cada vez más valioso sin que el ciudadano sea siempre consciente de ello. En consecuencia, la información, formación y uso de códigos tipo son cada vez más necesarios.

En definitiva, nos hallamos en el comienzo de una nueva etapa. Hay que abordar la defensa del derecho a la protección de DCP con los medios jurídicos de que se dispone y no parece suficiente ni adecuado dejar simplemente a la iniciativa privada la defensa del derecho fundamental a la protección de DCP. La solución adecuada para garantizar este derecho es tanto la intervención pública como la actuación privada, dirigiendo e impulsando la primera a la segunda Se precisan regulaciones acordadas internacionalmente que velen por una actuación coordinada en defensa del derecho a la autodeterminación informativa.

Palabras clave

autodeterminación informativa, datos de carácter personal, códigos tipo, intervención pública, autorregulación

Tema

Protección de datos

Perspectives on the right to informative self-determination

Abstract

The current situation of the Spanish legal system as regards data protection is, to a certain degree, contradictory. The fundamental right to data protection is acknowledged and a legal framework exists for its development, but the sectorial regulations covering this right are insufficient.

Within the public ambit, regulations exist – others are awaiting approval – that have direct implications for the processing of personal data (PD): some are only remitted to the Organic Law on Data Protection and others are somewhat contradictory to this Law. Whatever the case, the AEPD (Spanish Data Protection Agency) and the Courts will have to be especially rigorous in the application of this Law in order to protect not only the right to informative self-determination, but personal freedom itself. The private sector requires greater attention as it is not subject to institutional conditions, and citizens are not always aware of the fact that PD constitutes an increasingly valuable asset. Consequently, information, training and use of model codes become increasingly necessary.

In short, we are at the advent of a new era. We must address the defence of our right to PD protection by using the existing legal resources, and it seems neither sufficient nor appropriate to leave the defence of our fundamental right to PD protection solely to private initiative. The adequate solution for ensuring this right encompasses public intervention and private actions, directing and driving the former towards the latter. It is vital that we have internationally-agreed regulations that ensure a coordinated action in defence of our right to informative self-determination.

Keywords

informative self-determination, personal data, model codes, public intervention, self-regulation

Topic

Data protection

1. El actual estado de las cosas

El derecho a la autodeterminación informativa, objeto de esta sesión, ha sido reconocido, bajo la denominación de derecho a la protección de datos de carácter personal, en la Carta de los Derechos Fundamentales de la Unión Europea, figura, por tanto, incluido en el Tratado por el que se establece una Constitución para Europa, y se ocupan de garantizarlo el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de las Comunidades Europeas, cada uno en su respectivo ámbito de actuación. Varias sentencias de uno y otro se han pronunciado sobre él.

Por lo que se refiere al ordenamiento español, además de la proyección que tienen en su seno los textos mencionados y la jurisprudencia de esas instancias jurisdiccionales, sucede que ha sido reconocido como derecho fundamental por el Tribunal Constitucional (STC 292/2000) y, de ese modo, preside, da sentido y unifica una normativa cada vez más amplia, establecida a partir de 1992, primero por la Ley Orgánica 5/1992 (LORTAD) y, después, por la Ley Orgánica 15/1999 (LOPD). De acuerdo con lo previsto por esa legislación, desde 1994 contamos con la Agencia Española de Protección de Datos, institución independiente, encargada de velar por su observancia, que desarrolla una intensa labor de defensa especializada del derecho a la autodeterminación informativa, tarea en la que la acompañan, si bien solamente respecto de los ficheros y tratamientos de los órganos autonómicos y de las entidades locales correspondientes, otras agencias de ámbito territorial, hasta ahora, la madrileña, la catalana y la vasca.

A su vez, las normas vigentes son aplicadas por los tribunales ordinarios, que también controlan la actuación de las agencias mencionadas, así como las de los restantes poderes públicos. Y, con sus sentencias, van despejando algunos puntos oscuros de la legislación vigente en la materia y están sentando una interpretación que se caracteriza por orientarse, en general, a dotar de la mayor efectividad a este derecho.

Por tanto, el escenario que tenemos a la vista puede verse como el punto de llegada o la meta a la que apuntaban las iniciativas que, desde mediados de los años ochenta, reclamaban la protección frente al avance tecnológico, y muy particularmente frente al uso de la informática (Lucas Murillo de la Cueva, 1990). En efecto, esa defensa se ha configurado como el objeto de un nuevo derecho fundamental que ha cobrado carta de naturaleza en el marco de la Convención Europea para la Salvaguarda de los Derechos Humanos, en el ordenamiento comunitario y en el ordenamiento constitucional español. Además, si reparamos en el texto del Tratado por el que se establece una Constitución para Europa, veremos que no sólo reconoce como fundamental el derecho a la protección de datos de carácter personal, algo que ya hacía la Carta de Niza del 2000. Da un paso adicional e incluye su respeto entre los elementos de la vida democrática de la Unión Europea, dotándole también de este modo de una dimensión objetiva específica que refuerza su significación.

Una vez sentado lo anterior, ayudará a situar mejor lo que sigue recordar sumariamente en qué consiste este derecho.

Bastará para ello con tener presente que la protección de datos de carácter personal es un derecho fundamental autónomo que subyace al artículo 18.4 de la Constitución y tiene por objeto principal poner en mano de los individuos todos los medios jurídicos para controlar el uso por terceros de sus datos personales. Del mismo modo que uno de los sentidos de la palabra autodeterminación es el que apunta al ejercicio por cada uno de la propia libertad, ese término con el calificativo «informativa» indica definición o control por el afectado de la información que le concierne.

El control que nos ofrece este derecho fundamental descansa en dos elementos principales. El primero es el del consentimiento del afectado como condición de licitud de las actividades de captación y utilización de datos personales por terceros. Consentimiento inequívoco, libre e informado que permite a la persona a la que se refieren autodeterminarse informativamente. No obstante, es claro que en ciertas ocasiones ha de ser posible tratar información personal sin que medie la autorización del afectado. Por eso, y aquí viene el segundo elemento, la ley puede autorizarlo expresamente, bien de forma general, al darse las circunstancias por ella previstas, o caso por caso. Así, consentimiento y habilitación legal son los títulos que justifican el tratamiento de datos personales.

Ahora bien, que, por mediar cualquiera de ellos, sea lícito recogerlos y utilizarlos no significa que el afectado pierda su capacidad de autodeterminación en este ámbito. Al contrario, dispone de una serie de facultades –de derechos– que completan su poder de disposición y de control, empezando por el de revocar la autorización cuando la hubiere prestado. Facultades que tienen por objeto ejercer su poder de consentir el tratamiento de sus datos con pleno conocimiento de las consecuencias de su decisión y, luego, reaccionar contra quienes hagan un uso indebido de ellos.

Así, integran el contenido activo de este derecho las siguientes facultades: 1) ser informado en la recogida de datos; 2) conocer la existencia de ficheros y tratamientos de datos personales; 3) acceder a ellos para comprobar qué información personal del afectado contienen; 4) obtener la rectificación de los que no sean exactos; 5) obtener la cancelación de los que no deban ser tratados o hayan perdido la calidad que en su día justificó el tratamiento; 6) oponerse a un tratamiento cuando no sea necesario conforme a la ley el consentimiento del afectado y concurran motivos fundados y legítimos relativos a su concreta situación personal; 7) no sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente; 8) ser resarcido de los sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas; 9) ser protegido por las instituciones especializadas creadas *ex profeso* para defender este derecho fundamental.

A su vez, estas facultades constituyen el reverso de los deberes y obligaciones que pesan sobre quienes efectúan tratamientos de datos personales y, en último caso, sobre las agencias de protección de datos.

En fin, la tipificación como delito o infracción administrativa de las conductas que vulneran más gravemente el

derecho a la autodeterminación informativa completa su régimen jurídico esencial.

2. Las circunstancias que nos han traído hasta aquí

A este resultado se ha llegado como consecuencia de la convergencia de una pluralidad de factores.

Pueden variar en cada una de las experiencias nacionales los elementos que entran en juego así como las modalidades y términos del reconocimiento del derecho, pero son comunes, al menos, los siguientes: a) la creciente informatización de la sociedad en los países avanzados y el avance vertiginoso de las tecnologías de la información y de las comunicaciones (TIC); b) la circulación cada vez más intensa de personas, bienes y servicios, especialmente, pero no de modo exclusivo, en el seno de la Unión Europea; c) la virtualidad de esas tecnologías para canalizar relaciones de todo tipo dentro y fuera de los Estados; d) las posibilidades que ofrecen para la injerencia en la vida ajena por parte del poder público o de sujetos privados; e) la utilidad que representan como instrumento de control y de seguridad en manos de los gobernantes; f) el valor económico directo o indirecto que han adquirido los datos personales; g) la reivindicación desde diversos sectores, no mayoritarios y, preferentemente, intelectuales y comprometidos con los derechos humanos, de instrumentos de tutela jurídica contra los potenciales peligros que traen consigo esas tecnologías para las personas.

En España, la respuesta fue tardía en comparación con otros países que comenzaron a reaccionar frente a esos riesgos ya a principios de los años setenta. Y si después hemos avanzado con más rapidez, no se debe olvidar que la previsión efectuada por el artículo 18.4 de la Constitución permitía esperar una actuación del legislador más diligente y, sobre todo, debida a razones digamos de libertad. Sin embargo, lo que determinó el cumplimiento del mandato constitucional fue la incorporación de España al espacio previsto en los Acuerdos de Schengen y la correlativa exigencia de dotarse de una normativa de protección de datos personales. Pero, desde la Ley Orgánica 5/1992, hasta la Sentencia del Tribunal Constitucional 292/2000 que reconoce el derecho fundamental, se han sumado los siguientes elementos, cuya concurrencia explica el sentido de ese pronunciamiento:

1.º) El debate de intensidad creciente promovido desde ámbitos académicos y sociales sobre el bien jurídico que protegía esa legislación y, en particular, sobre la diferencia existente entre intimidad y autodeterminación informativa.

2.º) La progresiva elaboración en el espacio europeo, a partir del Convenio del Consejo de Europa n.º 108, de una disciplina orientada a proteger los datos personales, que acabará plasmada en la Directiva 95/46.

3.º) El paso dado por la Unión Europea en el 2000 con la Carta de los Derechos Fundamentales al reconocer la autonomía del derecho a la protección de datos de carácter personal.

4.º) La jurisprudencia del Tribunal Europeo de Derechos Humanos que, a partir del derecho a la vida privada reconocido por el artículo 8 de la Convención, dotó de autonomía a la protección de datos de carácter personal (casos Amann contra Suiza y Rotaru contra Rumania, ambos del 2000).

5.º) La dinámica generada por la aplicación de una Ley –la LORTAD– que expresamente hablaba de un nuevo derecho fundamental, y por la jurisprudencia constitucional que, en sintonía con posiciones doctrinales, iba acentuando la autonomía de la técnica jurídica de la protección de datos personales respecto del derecho a la intimidad.

Bajo todas estas premisas, la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, interpretando el artículo 18.4 de la Constitución, a la luz del Convenio n.º 108 del Consejo de Europa, conforme lo quiere el artículo 10.2, también del texto de 1978, dio el paso de reconocer el derecho fundamental a la protección de datos de carácter personal, opción cuya importancia es manifiesta y que, más allá de su decisivo significado jurídico, destacado por todos los intérpretes, ha merecido algunas críticas, sea por el lugar en que ha asentado ese derecho fundamental (el citado artículo 18.4), sea por los términos en los que lo ha reconocido (Martínez Martínez, 2004).

En definitiva, los riesgos del avance tecnológico, el diálogo entre la doctrina, el legislador y los jueces, así como el trasfondo europeo, junto a la virtualidad de la interpretación constitucional (Lucas Murillo de la Cueva, 2003) explican que hayamos llegado hasta aquí y, también, que

vayamos conociendo cada vez mejor las distintas facetas y aspectos del derecho a la autodeterminación informativa, entre ellos sus conexiones y diferencias con otros derechos fundamentales, particularmente, con los que se sitúan en el plano más próximo a la personalidad.

3. Las perspectivas

Los progresos que se van dando en materia de derechos son ciertamente conquistas importantes, pero, una vez alcanzados, se convierten en el punto de partida para lograr nuevos retos, nuevas aspiraciones. Por otro lado, el reconocimiento de un derecho por sí mismo no basta para asegurar su efectiva realización. Estas observaciones, válidas con carácter general, sirven también en relación con el derecho a la protección de datos de carácter personal. Son, incluso, especialmente significativas porque ha sido alumbrado recientemente y porque guarda relación estrecha con un proceso de transformación de las relaciones sociales a impulsos del progreso tecnológico que está en plena materialización.

Resulta, a propósito de lo primero, que las leyes, al menos las dictadas en España, han trazado un marco general de protección de datos que, si bien tiene la ventaja de contar con normas abiertas susceptibles de ser aplicadas a una multiplicidad de supuestos de hecho, en cambio, tiene que afrontar la dificultad que representan las particularidades de algunos ámbitos especialmente complejos, necesitados, por tanto, de una consideración singular, con la que no contamos. Por citar algún ejemplo, cabe mencionar, en ese sentido, el régimen de los ficheros y tratamientos de datos de carácter personal de los juzgados y tribunales, sobre el que hay una sucinta previsión legal (los artículos 230 y 235 de la Ley Orgánica del Poder Judicial) y una insuficiente regulación reglamentaria (recogida en el Reglamento sobre aspectos accesorios de las actuaciones judiciales) que propicia algunas controversias que, de otro modo, no se plantearían (SSTS de 18 y 19 de septiembre y de 30 de octubre de 2006 –recursos 74/2003, 274/2002 y 183/2003, respectivamente–).

Asimismo, se ha insistido en la falta de coordinación existente entre las normas que regulan la protección de datos de carácter personal y las dedicadas por la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, al acceso a los registros y archivos públicos previsto por el artículo 105 b) de la Constitución. Aspecto éste que adquirirá nuevos perfiles cuando entre en vigor la Ley para el Acceso Electrónico de los Ciudadanos a las Administraciones Públicas, actualmente pendiente de aprobación por el Congreso de los Diputados. Y también se ha llamado la atención sobre la necesidad de contar con previsiones que tengan en cuenta las características de los datos relativos a la educación y a la enseñanza, ámbitos en los que se han producido algunos conflictos a propósito de la publicación de calificaciones de los alumnos y de las evaluaciones de la labor docente e investigadora de los profesores universitarios (Troncoso Reigada, 2006).

Problemas que ha querido resolver la Ley Orgánica 4/2007, de modificación de la de Universidades, que autoriza la publicación de las calificaciones de los alumnos y de los resultados de la evaluación de la labor docente e investigadora de los profesores, al tiempo que requiere al Gobierno para que regule los *currículum* de profesores e investigadores. Por su parte, la Ley Orgánica 2/2006, de Educación, ha establecido algunas previsiones específicas en su disposición adicional vigésimo tercera, sobre el tratamiento de los datos de los alumnos. Una y otra se remiten, por lo demás, al régimen general establecido por la LOPD.

Hasta hace relativamente poco tiempo, otro de los sectores para los que se reclamaban reglas específicas era el de los *datos relativos a la salud*. No obstante, la Ley 41/2002, básica reguladora de la autonomía del paciente, afrontó ese problema, aunque su regulación suscite algunos interrogantes de importancia.

Consideraciones no muy distintas habría que hacer respecto de algunos ficheros y tratamientos realizados por sujetos privados. Sería el caso de los que se llevan a cabo en el ramo de los seguros, la *solvencia y crédito* o en el marco de las *relaciones laborales*.

Ahora bien, la solución a la que está recurriendo el legislador cuando contempla la cuestión de la protección de datos en campos específicos (órganos jurisdiccionales, telecomunicaciones, servicios de la sociedad de la información, firma digital, educación, universidades) ha consistido, fundamentalmente, en remitirse a la ley general sin aportar más que algunas previsiones muy concretas, aunque puedan ser muy relevantes, como especificar algunos derechos y atribuir potestad sancionadora a la Agencia Española de Protección de Datos en materia de servicios

de la sociedad de la información y comercio electrónico (Ley 34/2002) y de telecomunicaciones (Ley 32/2003).

A lo que se ha dicho, debe añadirse que lo reciente y lo novedoso de la materia implica desconocimiento de su importancia no sólo por los ciudadanos, sino también por quienes están al frente de las instituciones. Esto último es particularmente grave porque, a casi quince años de la publicación de la Ley Orgánica 2/1992, no puede considerarse satisfactorio el cumplimiento por parte de las administraciones de las exigencias propias de la legislación sobre protección de datos o que no se haya procedido a dictar los reglamentos de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal y permanezcan en vigor los aprobados conforme a la LORTAD, a pesar de que han transcurrido ya más de siete años de la derogación de ésta por aquélla.

Y, si esto sucede con los poderes públicos que están doblemente vinculados por la Ley, positiva y negativamente, se debe comprender que los ciudadanos desconozcan todavía los riesgos a que se exponen como consecuencia del uso por terceros de sus datos personales y, por tanto, no tengan conciencia de que deben luchar por los derechos que para su protección tienen reconocidos. Esa limitada lucha de los ciudadanos por los derechos de autodeterminación informativa hace que la labor de los Tribunales –y anteriormente de la Agencia Española de Protección de Datos– se vea condicionada por el relativamente escaso número de recursos –reclamaciones en el caso de la Agencia– que les llegan, aunque eso no les haya impedido dictar sentencias y resoluciones de gran importancia para abrir espacios, reforzar los límites de la actuación de las administraciones en relación con los datos personales y poner freno a abusos y excesos cometidos por particulares, empresas en especial, que se dedican a su tratamiento o se valen de los realizados por otros.

Las perspectivas que tenemos abiertas son, por tanto, contradictorias. De un lado, reflejan el aspecto positivo representado por la existencia de un reconocimiento del carácter fundamental del derecho, junto con un marco jurídico general europeo y estatal que lo desarrolla, así como por la actuación cada vez más eficaz de autoridades independientes de control y la tutela decidida prestada por los tribunales de justicia. Pero, de otro, expresan las insuficiencias relacionadas con la carencia de regulaciones sectoriales y la falta de una efectiva observancia de los principios y derechos de la autodeterminación informativa en muchos espacios. Y, en consecuencia, el enorme trabajo que queda por hacer para superar tal estado de cosas.

Estas consideraciones generales deben ser acompañadas por otras referidas separadamente al ámbito público y al privado, las cuales deben tener presente que las relaciones que tienen lugar dentro de cado uno y entre ellos se producen y se producirán, cada vez más, a través de medios electrónicos. A ese respecto, el fenómeno de Internet y de las otras formas o canales de comunicación que hacen posible las TIC suscitan problemas y dificultades de particular importancia en ambos planos.

4. El dominio público. La eficacia, la eficiencia y la seguridad

Mencionaba antes el Proyecto de Ley de Acceso Electrónico a las Administraciones Públicas, en avanzado estado de tramitación legislativa. Este proyecto contiene el reconocimiento del derecho de los ciudadanos a relacionarse con la Administración y recibir comunicaciones de ella por medios electrónicos. Al mismo tiempo, contempla la regulación del procedimiento administrativo por medios electrónicos y quiere que, para el 31 de diciembre del 2009, todas las administraciones –la Administración General del Estado, las autonómicas y las locales– estén en condiciones de hacer posible, en todos los procedimientos, el derecho a acceder electrónicamente a ellas.

Las posibilidades que la administración electrónica ofrece en términos de eficacia y eficiencia son evidentes. Como apunta la exposición de motivos del proyecto, no sólo servirán para superar o relativizar las barreras que suponen el tiempo y el espacio a la hora de obtener servicios públicos o de formular todo tipo de reclamaciones, sino que, a la vez, harán posible que los ciudadanos obtengan respuestas con una rapidez desconocida. De este modo, las administraciones ganarán un grado de cercanía efectiva del que ahora carecen. En este sentido, las aspiraciones del proyecto son muy ambiciosas y cuando se conviertan en realidad significarán un cambio cualitativo en la actuación de los poderes públicos en sus relaciones internas y externas. Cambio del que, en la actualidad, contamos con muestras elocuentes en aspectos que van más allá de la muy generalizada oferta de información, como es, por

ejemplo, la que ofrece la Agencia Estatal de la Administración Tributaria en relación con la declaración y liquidación de tributos (en virtud de lo previsto por la Ley General Tributaria).

No obstante, a las ventajas que ese objetivo comporta van unidas dificultades de entidad. El proyecto se remite a la LOPD en cuanto a la protección de los datos personales y, en coherencia con lo que en ella se dispone, exige el consentimiento del afectado o autorización legal para recabar de las distintas dependencias donde se hallen los documentos precisos, que el interesado, conforme al artículo 35 de la Ley 30/1992, no tiene por qué aportar. También limita su utilización al procedimiento de que se trate y exige que se observen las medidas de seguridad necesarias a la hora de la conservación y custodia del expediente electrónico. No contiene, sin embargo, criterios específicos sobre cesiones o comunicaciones de datos personales en las relaciones administrativas ni tampoco respecto del acceso por terceros a esos expedientes y a los registros electrónicos correspondientes. Sobre lo uno y lo otro habrá que estar a las normas de la LOPD y de la Ley 30/1992.

Se ha dicho que la exigencia de autorización legal para que, en ausencia de consentimiento del afectado, las administraciones puedan efectuar comunicaciones de los datos personales es un exceso en el que habría incurrido el Tribunal Constitucional al declarar la nulidad de la parte del artículo 21 de la LOPD, que consideraba suficiente para ello que lo previera la disposición de creación del fichero o, en general, una norma reglamentaria. No estoy seguro de que quepa tachar de exceso ese pronunciamiento. En cambio, sí que me parece conveniente imponer límites estrictos a las administraciones respecto del uso de los datos de que disponen aunque sea para el ejercicio de las funciones que tienen conferidas. Asimismo, creo que las normas de la LOPD sobre el consentimiento y sobre aquellos otros supuestos en los que exime de su prestación expresa por considerarlo implícito, ofrecen un margen importante, al igual que lo suministran las distintas normas legales atributivas de potestades a esas administraciones. Desde uno y otro frente, debe obtenerse espacio suficiente para llevar a cabo las comunicaciones que sean imprescindibles.

En cuanto al acceso, no por el afectado, sino por terceros interesados a los expedientes, archivos y registros administrativos, la Ley 30/1992 lo circunscribe de manera que el respeto al derecho a la intimidad se convierte en uno de los límites al mismo. Y también excluye la solicitud de acceso genérica o generalizada, al tiempo que restringe ese acceso por terceros a documentos nominativos que, sin referirse a aspectos íntimos, contengan datos de carácter sancionador o disciplinario a quienes lo pretendan para el ejercicio de un derecho, siempre que acrediten un interés legítimo y directo. Los cuales deberán solicitarlo individualmente, pudiendo ser denegado, motivadamente, además de cuando lo prevea la Ley, en los casos en que deban prevalecer razones de interés público o derechos de terceros más dignos de protección. Normas todas éstas que vienen siendo precisadas por la jurisprudencia que ha admitido, por ejemplo, como no lesivo del derecho a la autodeterminación informativa el traslado del expediente a los interesados que son parte en un procedimiento administrativo [STS de 26 de octubre de 2005 (casación 5173/2001)] o el acceso a los ejercicios de otros aspirantes en procedimientos competitivos para el ingreso en las administraciones públicas [STS de 6 de junio de 2005 (recurso 68/2002)]. Y ha rechazado pretensiones de acceso masivas o genéricas [STS de 19 de mayo de 2003 (casación 3193/1999)].

De esta manera, siguiendo criterios razonables y atendiendo a las previsiones legales, el espacio que queda es menos amplio de lo que pudiera parecer. Por otro lado, cabe considerar que el artículo 37 de dicha ley ofrece el soporte legal necesario para consentir un acceso puntual por terceros a datos personales de otros y que, incluso, suministra a las administraciones públicas fundamento para delimitarlo. Esta impresión no es compartida, sin embargo, por quienes opinan, con argumentos respetables –entre ellos el que apunta al distinto peso de un derecho fundamental y de un interés legítimo–, que es imprescindible abordar una regulación que armonice satisfactoriamente el derecho a la autodeterminación informativa con el de acceder a los archivos y registros públicos (por ejemplo, Fernández Salmerón, 2003).

Con todo, no me parece que los problemas más graves vengan desde esta dirección. Me parecen más preocupantes los que tienen que ver con el cumplimiento real de las medidas de seguridad, con poner término a los accesos y comunicaciones ilegales de datos o con evitar procedimientos de eliminación de documentación consistente en arrojar a la basura expedientes completos o historias clínicas. En este plano, la formación de los funcionarios es imprescindible, de igual modo que la exigencia de responsabilidad disciplinaria siempre que proceda.

Asimismo, me parece importante prevenir e impedir excesos con el pretexto de la protección de la seguridad pública. El afán por acopiar por todos los medios disponibles información relevante para combatir, sobre todo, el terrorismo se ha hecho sentir con gran fuerza después del 11 de septiembre de 2001 y ha llevado a que, especialmente en Estados Unidos, se hayan creado bases de datos de carácter personal que incluyen, incluso, los de carácter sensible, y son gestionadas al margen de todo sistema de control efectivo por parte de los afectados o de instancias independientes. Un ejemplo del que han venido informando los medios de comunicación es el relativo a la recopilación en secreto de datos financieros y de transacciones bancarias de ciudadanos de diversas nacionalidades a partir de una empresa belga que canaliza diariamente millones de operaciones bancarias mediante un programa denominado Swift, operado por el Departamento del Tesoro (*New York Times* de 23 de junio del 2006). Y también se puede mencionar el programa de vigilancia sobre las telecomunicaciones Echelon.

El riesgo de la utilización de los ingentes recursos que las nuevas tecnologías ofrecen a este respecto se ha proyectado, incluso, en controversias que han llegado a plantearse jurisdiccionalmente, como es el caso de los datos personales sobre pasajeros de líneas aéreas que viajan a América del Norte que han de ser suministrados a la Administración estadounidense. Conflicto al que se le dio una solución que no todos vieron como satisfactoria desde el punto de vista del ordenamiento comunitario en materia de movimientos internacionales de datos personales, luego anulada por la Sentencia de 30 de mayo de 2006 del Tribunal de Justicia de las Comunidades Europeas si bien por motivos de carácter competencial y, por tanto, ajenos al derecho a la autodeterminación informativa. En la actualidad la cuestión está pendiente de la negociación de un nuevo acuerdo entre Estados Unidos y la Unión Europea.

Otro plano en el que se han suscitado interrogantes es el que tiene que ver con la introducción de *nuevas obligaciones para las empresas que prestan servicios de telecomunicaciones* sobre las llamadas que realicen sus abonados. Iniciativas que van en la línea de las medidas ya previstas en ese sentido por el artículo 12 de la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico, para operadores de redes y servicios, proveedores de redes de acceso a telecomunicaciones y prestadores de servicios de alojamiento de datos, que les obligan a retener y conservar durante doce meses los de conexión y tráfico de comunicaciones realizadas durante la prestación de un servicio de los contemplados por ese texto legal. Previsión legal que se preocupa, no obstante, de precisar que, en ningún caso, se extiende esa obligación al contenido de las comunicaciones.

La Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), se limitó a autorizar a los Estados a obligar, por ley y para proteger la seguridad nacional y la seguridad pública, entre otras razones, a conservar por un plazo determinado los datos personales relativos a las comunicaciones electrónicas (artículo 15.1). Pero la Directiva 2006/24, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, la ha modificado en parte y ha desarrollado este aspecto.

Responde a la necesidad de armonizar las legislaciones estatales en la materia ante el crecimiento de las comunicaciones electrónicas y la necesidad de combatir la delincuencia organizada y, particularmente, el terrorismo. No en vano, tras los atentados de Londres de julio del 2005 se anunciaron por diversos gobernantes medidas del tipo de las ahora adoptadas y en los considerandos de este texto se hace referencia expresa a ellos. Es de destacar que la regulación recogida en esta nueva directiva parte del mismo principio ya adoptado para las comunicaciones relativas al comercio electrónico: la obligación de conservar los datos no se refiere al contenido de la comunicación sino solamente a aspectos externos a ella. Es decir, a los generados o tratados en el proceso del suministro de servicios de comunicación. Más en concreto, se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los relacionados necesarios para identificar al abonado o al usuario registrado. Y quedan incluidos los correspondientes a las llamadas infructuosas. El período de conservación se fija entre seis meses y dos años, ampliables si median circunstancias especiales, durante el cual podrán acceder a esta información las autoridades competentes, conforme a la legislación de cada Estado.

Es el legislador estatal quien ha de regular los términos concretos en los que la información relativa a las comunicaciones ha de ser conservada y de qué manera podrán acceder a ella las autoridades competentes. La directiva,

consciente de lo delicado de esta materia, le hace advertencias explícitas y reiteradas sobre los extremos que debe tener presente al realizar esa tarea. En efecto, advierte que ese acceso solamente podrán realizarlo dichas autoridades respetando los derechos fundamentales de las personas afectadas y observando el principio de proporcionalidad. Igualmente, demanda medidas de seguridad para evitar que accedan quienes no deban a estos datos, y requiere sanciones para quienes lo hagan indebidamente. De igual modo, asegura el derecho al resarcimiento, conforme a la Directiva 95/46 a quienes sufran como consecuencia de tratamientos ilícitos o de acciones incompatibles con las legislaciones internas que han transpuesto esa directiva.

La preocupación que expresa la directiva por circunscribir los márgenes en los que ha de moverse el legislador interno ya nos advierte de que detecta serios riesgos en las medidas de conservación y puesta a disposición de las autoridades competentes de estos datos. Y eso a pesar de que quedan excluidos expresamente los relacionados con el contenido de las comunicaciones. Pero los vinculados al origen y destino (intervinientes), fecha, hora y duración, tipo de comunicación, equipo de los usuarios y su localización son suficientemente significativos desde la perspectiva no sólo del derecho a la autodeterminación informativa sino de otros derechos fundamentales como para despertar las alarmas.

Naturalmente, esto significa que habrá que examinar con el mayor cuidado la forma en que las Cortes Generales van a transponer al ordenamiento español esta directiva. El proyecto de ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, actualmente en trámite en el Congreso de los Diputados se dirige a tal fin (Boletín Oficial de las Cortes Generales. Congreso de los Diputados, Serie A, n.º 128-I, de 16 de marzo de 2007). Lo delicado de la materia lo reconoce el propio texto, que se preocupa por resaltar reiteradamente que queda a salvo de las medidas que contempla el contenido de las comunicaciones y que las cesiones de los datos que obliga a conservar solamente se producirán con autorización judicial. Ahora bien, eso no le impide extender la obligación de cederlos, aunque sea con esa garantía, a los relevantes para la investigación de cualquier delito y no sólo de los graves, que es lo que considera la directiva. La exposición de motivos del proyecto explica que esa extensión está permitida por la directiva, guarda relación con el régimen del secreto de las comunicaciones y es aconsejable, ya que, muy a menudo, cuando comienza una investigación criminal no se percibe el alcance que llegará a tener y que, de este modo, no se cercenan las posibilidades puestas a disposición de la autoridad judicial para detectar las responsabilidades penales.

El articulado precisa que los obligados a conservar los datos son los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (artículo 2), indica los datos que deben ser conservados en los términos previstos por la directiva (artículo 3), incluyendo los relativos a las llamadas infructuosas (artículo 4) y durante cuánto tiempo: doce meses, plazo que reglamentariamente puede ampliarse hasta dos años o reducirse hasta seis meses para determinados datos (artículo 5). En cuanto a la cesión (artículos 6 y 7), precisa que solamente cabe efectuarla, previa autorización judicial que determinará el alcance de la misma, a los agentes facultados y que éstos son (artículo 6.2)) los miembros de las Fuerzas y Cuerpos de Seguridad del Estado cuando actúen como policía judicial y los del Centro Nacional de Inteligencia en el curso de investigaciones sobre personas o entidades en el marco de lo previsto en la Ley 11/2002, de 6 de mayo, que lo regula y en la Ley Orgánica 2/2002, de la misma fecha, que regula el control judicial previo de sus actividades. También tendrán la consideración de agentes facultados los funcionarios de la Dirección Adjunta de Vigilancia Aduanera cuando actúen como policía judicial.

El plazo para efectuar la cesión, dice el proyecto, será fijado por los agentes facultados atendiendo a la urgencia y a la naturaleza y complejidad técnica de la operación. En todo caso, señala para los supuestos en los que no se fije el de cuarenta y ocho horas para datos de antigüedad inferior a tres meses y el de setenta y dos horas para los que la superen (artículo 7.3). La cesión se realizará en formato electrónico de acuerdo con las particularidades que deberán establecer conjuntamente en el plazo de tres meses desde la entrada en vigor de la ley los Ministerios de Interior, Defensa y Economía y Hacienda. Y correrá a cargo de los sujetos obligados la configuración de sus equipos y la actualización técnica necesarias para cumplir las obligaciones de conservación y cesión de datos (disposición final cuarta).

Completan las normas especiales incluidas en el proyecto las relativas a la protección y seguridad de los datos, las excepciones a los derechos de acceso y cancelación y las correspondientes a las infracciones y sanciones. En cuanto a lo primero, el artículo 8 efectúa varias remisiones a la LOPD y reitera que la Agencia Española

de Protección de Datos es la responsable de velar por su cumplimiento. Más importantes son las previsiones del artículo 9, que excluyen el deber de los responsables de los tratamientos de comunicar las cesiones y les obligan a denegar el ejercicio del derecho de cancelación a quien sea objeto de investigación de un delito o sus datos hayan sido cedidos conforme a lo previsto en esta normativa. Al mismo tiempo, reconocen a los afectados que vean denegadas en todo o en parte sus pretensiones de cancelación, el derecho a ponerlo en conocimiento de la Agencia Española de Protección de Datos, la cual deberá asegurarse de la procedencia o improcedencia de la denegación. Finalmente, en materia sancionadora, el proyecto se remite a la Ley 32/2003, varios de cuyos preceptos modifica la disposición adicional única.

Hay, además, otras novedades, como la aportada por la disposición adicional única del proyecto en materia de identificación de las personas que adquieran tarjetas de prepago para los servicios de telefonía móvil. Identificación que deberán efectuar los operadores que comercialicen esos sistemas de activación para lo cual se les exige llevar un libro-registro y conservar los datos correspondientes durante la vigencia de la tarjeta y hasta que transcurran los plazos previstos en el proyecto, así como cederlos a los agentes facultados. Obligaciones éstas cuyo incumplimiento se castiga también conforme a lo previsto en la Ley 32/2003, según la modificación que en ella se introduce.

Es pronto para avanzar un juicio preciso sobre este régimen añadido. Parece que, en lo sustancial, el proyecto se ajusta a la Directiva y que comparte con ella, como no podía ser de otro modo, la preocupación por mantener un equilibrio entre las intervenciones que introduce y las garantías del secreto de las comunicaciones y del derecho a la autodeterminación informativa. La opción por extender las nuevas obligaciones a todos los casos de investigaciones por delito, con independencia de que la autorice la directiva, no es, en mi opinión, especialmente significativa. Lo más importante será controlar la utilización de estos instrumentos para limitarla a aquellos supuestos en los que esté justificado su uso y asegurar que se observan los plazos de conservación y las medidas de seguridad de los datos para que, efectivamente, no acceda a ellos quien no deba y en ningún caso se aprovechen para fines distintos de los previstos legalmente. Para ello, la Agencia Española de Protección de Datos y los jueces deberán ser especialmente exigentes porque estas medidas pueden afectar, no ya al derecho a la autodeterminación informativa y al derecho al secreto de las comunicaciones, sino a la propia libertad de las personas.

Por eso, no está de más recordar que, en efecto, los poderes públicos deben velar por la seguridad de todos, especialmente frente a la amenaza terrorista y las formas de criminalidad organizada. Y que deben servirse para ello de todos los medios disponibles entre los que destacan por su eficacia los que suministran las tecnologías de la información y las comunicaciones y permiten acopiar datos personales. Pero, al mismo tiempo y con el mismo énfasis, ha de tenerse presente que una cosa es que se sirvan de ellos para prevenir los delitos y perseguir a los delincuentes y otra distinta que procedan a registrar y tratar al margen de todo control la vida y obras de millones de personas sin relación alguna con tales conductas. La legislación vigente no lo permite. De lo que se trata es de que siga siendo así y de que cambios normativos, como el que está en ciernes y los que se puedan introducir en el futuro, si las circunstancias los exigieren, se hagan dentro del más estricto respeto a los principios que rigen, no ya en esta materia, sino, en general, en relación con los derechos y libertades de los ciudadanos. Para ello, no basta con el cuidado del legislador ni con el celo del gobernante. Es decisiva la vigilancia de los órganos e instituciones de garantía sobre quienes están encargados de aplicar las leyes.

Decía que, hasta ahora, no se han suscitado especiales problemas a propósito de los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado. Incluso, pueden apuntarse episodios que han puesto de manifiesto un buen funcionamiento del sistema de garantías creado por el legislador en este ámbito, como sucedió con la Circular 1/1997 de la Dirección General de Policía que dictaba instrucciones sobre «Captación de datos de interés para la Seguridad Ciudadana» (Del Castillo Vázquez, 2007). Según ellas, la Policía debía hacerse con datos sin que mediaran elementos que hicieran pensar en la posibilidad de una actuación delictiva, bastando con la simple curiosidad o sospecha de los agentes. Asimismo, se mencionaban las fuentes de información potenciales (entidades vecinales, vecinos, comerciantes, familiares, empresas de seguridad privada) y se estimaban informaciones de interés aquellas relativas a inquilinos, locales frecuentados por menores en los que se consumían bebidas alcohólicas, vehículos que circulaban a determinadas horas por el barrio y que pudieran dedicarse al tráfico de drogas, anuncios de alquiler de viviendas y comportamientos de personas no habituales que hubieren llamado la atención de algún vecino.

Esa circular suscitó críticas desde una asociación judicial y originó una pregunta en el Senado, ante lo cual el Ministerio del Interior optó por retirarla aduciendo en justificación de esa decisión su «redacción confusa» y que «su aplicación podría hacer llegar a la conclusión de que se estaban vulnerando determinados conceptos unidos al derecho fundamental a la protección de la intimidad».

En definitiva, no debe perderse de vista la idea central de que la mejor manera de defender los principios del estado de derecho, del que forman parte inescindible los derechos fundamentales, es respetándolos también a la hora de hacer frente al terrorismo y a la delincuencia organizada, lo cual exige observar escrupulosamente los procedimientos constitucionales que permiten limitarlos y los márgenes en los que es posible hacerlo. La supresión de las garantías sin esas cautelas o, en general, la creación de espacios inmunes al control parlamentario y judicial, a la larga solamente conduce a resultados contrarios a los perseguidos.

5. El dominio privado

Al estudiar la LORTAD me llamó la atención la amplitud de las excepciones que establecía en relación con el tratamiento de datos personales desde ficheros de titularidad pública (Lucas Murillo de la Cueva, 1993). Años más tarde (Lucas Murillo de la Cueva, 2000), tuve la impresión de que la LOPD, no sólo no corrigió esa disposición permisiva respecto de los poderes públicos, sino que la acompañó con la apertura de huecos a través de los que operadores privados podrían hacerse con datos de carácter personal y tratarlos sin consentimiento del afectado o más allá de los términos en los que éste fue concedido. Pensaba, sobre todo, en el cambio introducido en el artículo 4.2 de la LOPD, que permite utilizarlos para *finalidades distintas* de las que motivaron su recogida siempre que no sean incompatibles con él –la LORTAD prohibía su uso para fines distintos– y en la figura del *censo promocional*, fuente accesible al público, anunciada por la Ley 7/1996, de Ordenación del Comercio Minorista, que hace posible sortear la prohibición de acceso y utilización de los datos del censo electoral (artículo 31 LOPD).

Afortunadamente, el Tribunal Constitucional ha eliminado los excesos más llamativos con los que el legislador ha querido facilitar el tratamiento de datos personales por parte de las administraciones públicas (STC 292/2000) declarando la nulidad, por inconstitucionales, de parte de los artículos 21.1 (comunicación de datos entre administraciones públicas) y 24 (información en la recogida de datos y ejercicio de los derechos de acceso y rectificación ante los ficheros de titularidad pública). Por lo que se refiere a las mencionadas normas pensadas para facilitar los tratamientos desde el sector privado, aunque permanecen vigentes, la Audiencia Nacional y el Tribunal Supremo –que viene confirmando su interpretación de la LOPD– han reducido a la inoperatividad ambos cambios aportados por el legislador de 1999.

El primero, porque ha venido a equiparar las finalidades incompatibles con las diferentes a la que justificó la captación de los datos [SAN de 8 de febrero de 2002 (recurso 1067/2000, seguida posteriormente por otras)]. El segundo, porque ha negado virtualidad al artículo 39.3 de la Ley 7/1996, de Ordenación del Comercio Minorista, para hacer accesibles los datos del censo electoral, cuya prohibición de tratamiento mantiene en tanto la Ley Orgánica del Régimen Electoral General no disponga otra cosa [recientemente, STS de 7 de marzo de 2006 (casación 1728/2002), que recoge otras anteriores a partir de la STS de 18 de octubre de 2000]. Asimismo, en otros puntos estrechamente relacionados con el tratamiento de datos por sujetos privados, la jurisprudencia está siendo especialmente rigurosa. Es lo que sucede en cuanto a la exigencia del *consentimiento*, que no permite entenderlo concedido por la falta de manifestación del afectado en sentido contrario tras la comunicación de un sujeto privado de que se propone tratar sus datos de no recibir comunicación en contra [STS de 18 de marzo de 2005 (casación 7707/2000)]; y de la *finalidad determinada*, que excluye la validez de las formuladas en términos genéricos [STS de 11 de abril de 2005 (casación 4209/2001)]. O cuando limita a sus estrictos términos legales el concepto de *fuente accesible al público* [STS de 20 de febrero de 2007 (casación 732/2003)] y exige que los responsables de los ficheros y tratamientos velen por la *calidad de los datos*, depurando los inexactos y no puestos al día [STS de 18 de julio de 2006 (casación 322/2005)].

No obstante, esa proclividad del legislador hacia el sector privado me parece preocupante. Y es que, al fin y al cabo, el ámbito o dominio público está sujeto a límites y restricciones que no vinculan a los particulares. Eso explica que, a veces, sin necesidad de recurrir a los remedios especiales previstos por la LOPD, sino mediante los instrumentos ordinarios de control de la actuación del poder ejecutivo, es decir, haciendo efectivas las exigencias a las que la ley

somete la producción de actos administrativos o la elaboración de disposiciones generales, sea posible eliminar aquellos que se consideren contrarios al derecho que examinamos. Así, la STS de 28 de marzo de 2007 (recurso 76/2005), declaró la nulidad de los artículos 323.1 y 2 y 324 del Reglamento del Registro Mercantil (Real Decreto 685/2005) sobre publicidad vía Internet de resoluciones judiciales sobre deudores concursados por falta de dictamen del Consejo de Estado sobre la redacción finalmente aprobada. Y, desde el punto de vista de los controles parlamentarios, el caso antes relatado de la Circular 1/1997 de la Dirección General de la Policía muestra otro medio, no especializado, de limitar la acción pública en defensa también del derecho a la autodeterminación informativa.

En el ámbito privado, en cambio, esas restricciones y condicionamientos jurídicos e institucionales no existen. Y, sin embargo, los datos de carácter personal constituyen un bien cada vez más valioso económicamente por las posibilidades que su conocimiento y su elaboración ofrecen para las más variadas actividades. Eso hace que se demanden con creciente intensidad y que se redoblen los esfuerzos por captarlos y someterlos a tratamientos que lleven a un conocimiento más específico de las personas a las que pertenecen. Captación que no siempre se hace informando al afectado sobre los términos en los que se le pide el consentimiento, si es que se le solicita. Y tratamientos que pueden no respetar la finalidad que originó la recogida de unos datos determinados. Además, es un mundo mucho más opaco. Quiero decir que los actores que se mueven en él no hacen ostentación de la disposición de esa información personal, simplemente, la utilizan.

Si a esto unimos todo cuanto antes se decía sobre la todavía escasa conciencia de los peligros relacionados con la utilización por terceros de información personal y con el deficiente conocimiento de los instrumentos jurídicos pensados para proteger a los afectados, nos podremos hacer una idea más cabal de la entidad de los problemas que tenemos ante nosotros. Especialmente, en un contexto donde, sea a través de la televisión interactiva, la telefonía o Internet, los particulares exponen datos que les conciernen ante muy variados operadores, que pueden hacerse con ellos con gran facilidad sin que el usuario lo perciba.

No hay duda de que la Agencia Española de Protección de Datos es consciente de todo esto y que se esfuerza en advertir de los riesgos que implican el acceso y tratamiento incontrolados de datos personales por terceros y en informar sobre los medios para impedirlos. En este sentido, no hay duda de que lleva y ha llevado a cabo actuaciones muy importantes en relación con los ficheros de solvencia y crédito. Se han plasmado, además de en su labor inspectora y sancionadora, en la Instrucción 1/1995, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito [cuya legalidad ha confirmado la STS de 16 de febrero de 2007 (casación 220/2003)].

No obstante, la tarea que tiene por delante, a pesar del tiempo transcurrido desde el comienzo de su actuación (ya trece años), es ingente. Episodios semejantes a los descritos en relación con las administraciones públicas han tenido como protagonistas a empresas privadas, como, por ejemplo, arrojar a la basura informes elaborados sobre los aspirantes a un empleo. E incluso cabe pensar que, si entidades particulares han llegado a tratar datos sensibles sin pedir el necesario consentimiento –como los relativos a la afiliación política [STS de 25 de enero de 2006 (casación 7396/2001)] o a las creencias [STS de 17 de abril de 2007 (casación 3755/2003)]– o que no se han preocupado por dotarles de las imprescindibles medidas de seguridad, eso se debe en buena parte a que quienes protagonizan esos hechos no tienen pleno conocimiento no ya de su prohibición, sino de lo delicado del material que utilizan, aunque eso no les exima de afrontar la responsabilidad que hayan contraído con su comportamiento.

Y aquí vuelven a ser decisivas la información y la formación en protección de datos de carácter personal, así como el estímulo a la elaboración y al uso de códigos tipo, y, desde luego, la detección de las infracciones y el castigo riguroso a quienes las cometen. Tarea que ha de desarrollarse con especial energía ante la cada vez más intensa penetración de medios como Internet, la telefonía y la televisión interactiva en todas las facetas de la vida. En este sentido, lo dispuesto en el artículo 14.3 de la Directiva 2002/58 ofrece un campo de actuación que no siempre se tiene presente y que, sin embargo, posee una enorme importancia: el de la adopción de las medidas necesarias para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales. La propia Directiva 2002/58, en sus considerandos 24.º y 25.º, explica con claridad los problemas que para la protección del derecho a la autodeterminación informativa plantean los programas espías y, en general, los dispositivos ocultos que pueden introducirse en el equipo terminal del usuario y suministrar información

sobre él, extremos estos sobre los que se extiende la intervención del profesor Yves Poullet en esta misma sesión.

Problemas sobre los cuales, la Ley 32/2003, General de Telecomunicaciones, que ha transpuesto la directiva, no ha aportado soluciones.

Recientemente, el 1 de marzo del 2007, el Garante para la Protección de los Datos Personales de Italia ha aprobado una instrucción sobre *la utilización del correo electrónico e Internet en el marco de la relación de trabajo*. En ella se ocupa de sentar los criterios que han de observar los empleadores, públicos y privados, para organizar el uso que sus trabajadores hacen a través de los equipos de la empresa de esos medios de comunicación. Insiste especialmente en la protección de los datos personales de los empleados, ya sean los que puedan ser captados cuando realizan el trabajo que les corresponde, o los que tengan que ver con ellos mismos, y se detiene en los medios de control que puede disponer el empleador. En este sentido, prohíbe la lectura y el registro sistemático de los mensajes de correo electrónico o de la información sobre éstos más allá de cuanto sea técnicamente necesario para desarrollar el servicio, así como la reproducción y eventual memorización sistemática de las páginas web visualizadas por el trabajador. Igualmente, prohíbe la lectura y el registro de los caracteres introducidos desde el encabezamiento o análogo dispositivo y el análisis oculto de ordenadores portátiles puestos a su disposición.

Pues bien, éste es otro terreno en el que es preciso avanzar criterios claros por la proyección prácticamente general de la relación de empleo y porque ha suscitado problemas sobre los que no se ha llegado a establecer reglas precisas, lo que ha propiciado decisiones judiciales oscilantes.

La labor por realizar no es, ciertamente, una tarea que pueda enfocarse aisladamente desde un solo país, precisamente por la propia naturaleza de las formas de comunicación electrónica y de su capacidad para operar por encima de las fronteras. Precisamente por esa razón, la Directiva 95/46 ha erigido un sistema europeo de control que ha de ser fortalecido. Al mismo tiempo, a partir de la importante plataforma que ofrece la Unión Europea, es necesario intensificar todos los esfuerzos posibles para forjar acuerdos internacionales que extiendan las normas y las instituciones ideadas para proteger este derecho fundamental, de manera que no queden lugares vacíos de regulación en los que puedan encontrar refugio quienes pretenden aprovecharse de la información personal en beneficio propio y en desprecio del perjuicio que causan a los afectados.

6. A modo de conclusión

Nos encontramos en el comienzo de una nueva etapa. Una vez sentadas las bases constitucionales, legislativas e institucionales del derecho a la autodeterminación informativa, es menester abordar su decidida defensa con los medios jurídicos de los que ya se dispone. Es como pasar de la teoría a la práctica, de la norma a la realidad, tomando en serio los peligros que acechan y la relevancia del bien jurídico amenazado.

En ese empeño, no hay que olvidar que el derecho a la autodeterminación informativa es un derecho fundamental. Que se dirige a satisfacer una necesidad básica de toda persona: el control de la información que le concierne. Que no consiste en una exquisitez jurídica ni en un capricho, sino en una pretensión esencial en la sociedad en la que vivimos. Sin ese control, sin los límites que comporta para los poderes públicos y para los sujetos privados, ya sean los gobernantes, ya sean las empresas u otras entidades privadas, contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que estará en peligro el libre desenvolvimiento de nuestra vida e, incluso, nuestra propia identidad.

No es, por tanto, una cuestión menor, sino todo lo contrario. Además, el nivel de las amenazas aumenta exponencialmente a medida que se refinan –con el concurso del vertiginoso avance tecnológico– las técnicas y procedimientos que permiten acceder a datos de carácter personal y elaborarlos. Por otro lado, no hablamos de un problema específico o localizado en uno o varios países, sino que tiene una proyección universal. Ciertamente, el problema no se presenta en todos los sitios con la misma intensidad, ya que guarda relación con el grado de desarrollo de la sociedad de que se trate; sin embargo, en las sociedades que participan de los niveles de desarrollo que son propios de las nuestras, se plantea con toda su fuerza. Y, en tanto quienes no lo han alcanzado aspiran a lograrlo, también lo irán viviendo de forma creciente, con independencia de que ya les esté afectando.

Los datos de carácter personal ofrecen a quienes disponen de ellos poder y dinero. Dos estímulos ante los que es muy difícil oponer barreras eficaces si los interesados, las instituciones y los Estados no actúan de manera firme para contenerlos. El derecho a la autodeterminación informativa es un instrumento que permite luchar contra los excesos en el uso por terceros de información personal para extender su capacidad de dominación o influencia sobre los titulares de esa información u obtener beneficios económicos a su costa o gracias a ellos. Y la lucha por el derecho de la que hablaba Ihering es también y, sobre todo, lucha por los derechos. Ésta es la primera condición para que sean respetados.

La singularidad de la batalla por la autodeterminación informativa estriba en que se trata de una empresa que debe ser afrontada en la misma escala en la que operan las amenazas que se ciernen sobre ella. Solamente con actuaciones concertadas internacionalmente será posible lograr resultados eficaces frente al fenómeno de Internet, dado que no descansa en una localización determinada, sino que constituye una red con una multiplicidad de puntos desde los cuales se puede operar hacia el resto del mundo. Ya decía antes que la Unión Europea ha puesto en marcha un mecanismo de control de ámbito comunitario. Se trata de extender ese modo de operar a espacios más amplios para llevar a ellos normas y mecanismos de control que las hagan efectivas.

Es una tarea difícil porque debe tener en cuenta que no siempre se comparten los mismos criterios sobre cómo ha de asegurarse la protección de los datos de carácter personal. Se ha hablado a ese respecto de una diferente cultura en Estados Unidos y en Europa. No obstante, aun dejando un margen relevante para la iniciativa de los particulares, la autorregulación y el juego de la competencia, me parece que el esfuerzo y la responsabilidad principal debe descansar en los Estados y en sus organizaciones, ya que los Estados son los protagonistas indiscutibles de la vida internacional y siguen siendo instrumento imprescindible para la organización de la convivencia pacífica de las sociedades. Aunque parezca paradójico, los derechos necesitan de los Estados y se resienten cuando éstos son débiles.

No creo que deba plantearse una disyuntiva entre la intervención pública y la actuación privada como opciones alternativas y excluyentes. Sí pienso, en cambio, que la segunda debe ser dirigida e impulsada por la primera, ya que el mercado y la sociedad por sí mismos, no generarán espontáneamente remedios eficaces y perceptibles para todos los individuos. Sucede algo parecido a lo que se planteó, en su momento, a propósito de los derechos de los consumidores y usuarios: la lógica de la competencia no es suficiente para poner coto a las prácticas abusivas. Son, pues, necesarias regulaciones acordadas internacionalmente e instituciones del mismo carácter que velen por la actuación coordinada y coherente de las autoridades estatales encargadas de servir a modo de una primera línea de defensa especializada del derecho a la autodeterminación informativa.

Sólo contando con un marco normativo e institucional internacional con el que guarden coherencia y coordinación los propios de los Estados, será posible estimular y aprovechar las iniciativas que se mueven en el plano de la sociedad. La competencia y las buenas prácticas serán verdaderamente funcionales cuando se vean apoyadas por un ordenamiento preciso, sancionando con castigos rigurosos a sus infractores. Evitar multas y condenas es un buen acicate para buscar formas de actuación cuya observancia sea respetuosa con el derecho a la autodeterminación informativa. Sin esa referencia última, la espontaneidad y la autonomía privadas únicamente ofrecerán soluciones parciales y no siempre homogéneas, como, sin embargo, deben ser las dirigidas a hacer efectiva la protección de los datos de carácter personal.

Referencias bibliográficas

DEL CASTILLO VÁZQUEZ, Isabel Cecilia (2007). *El «habeas data»: aspectos constitucionales y administrativos (El derecho a saber y la obligación de callar)*. Tesis Doctoral. Madrid: Universidad Complutense.

FERNÁNDEZ SALMERÓN, Manuel. (2003). *La protección de datos personales en las Administraciones Públicas*. Madrid: Civitas.

LUCAS MURILLO DE LA CUEVA, Pablo (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

LUCAS MURILLO DE LA CUEVA, Pablo (1993). *Informática y protección de datos*. Madrid: Centro de Estudios Constitucionales.

LUCAS MURILLO DE LA CUEVA, Pablo (2000). «Las vicisitudes del Derecho de la protección de datos personales». *Revista Vasca de Administración Pública*. N.º 58-II. Pág. 211 y sig.

LUCAS MURILLO DE LA CUEVA, Pablo (2003). «La Constitución y el derecho a la autodeterminación informativa». Cuadernos de Derecho Público. N.º 19-20, pág. 27 y sig.

MARTÍNEZ MARTÍNEZ, Ricard (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas.

TRONCOSO REIGADA, Antonio (2006). «La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las Universidades». *Revista de Derecho Político*. N.º 67, pág. 79-163.

Cita recomendada

LUCAS MURILLO DE LA CUEVA, Pablo (2007). «Perspectivas del derecho a la autodeterminación informativa». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

‹http://www.uoc.edu/idp/5/dt/esp/lucas.pdf›

ISSN 1699-8154

Sobre el autor

Pablo Lucas Murillo de la Cueva

Magistrado del Tribunal Supremo (2001). Catedrático de Derecho Constitucional (1989). Autor, entre otras publicaciones, de los libros: *Informática y protección de datos personales* (CEC, Madrid, 1993); *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática* (Tecnos, Madrid, 1990).