INFORME "El tiempo de los derechos", núm. 26.

EL IMPACTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN EN LOS DERECHOS

EQUIPO DE INVESTIGACIÓN: GRUPO HI13 de la Universidad de Vigo. Laboratorio "Sociedad de la información y derechos humanos"

Fecha de elaboración: noviembre 2011

Fecha de publicación: septiembre 2012

1. Las tecnologías de la información y de la comunicación (TIC) han supuesto, por una parte, grandes ventajas y beneficios, tanto para las personas como para las empresas y Administraciones Públicas, en orden a facilitar sus objetivos, personales o profesionales, o sus funciones, puesto que permiten su realización de una manera más eficiente y rápida. Por otra parte, el desarrollo de estas tecnologías ha acarreado nuevos riesgos para los derechos y libertades de las personas debido a la capacidad de las entidades, tanto públicas como privadas, de acumular informaciones personales en formato digital para finalidades muy diversas y no siempre perfectamente identificadas. La pérdida de control sobre estas informaciones puede incidir de manera directa en los derechos y libertades ya que esta capacidad de acumulación de grandes cantidades de datos personales hace posible su alteración, manipulación y transmisión a terceros de manera rápida y a un bajo coste, lo cual incide en la libertad de elección y decisión de los individuos ante la incertidumbre de si sus comunicaciones, actividades o elecciones serán registradas por entidades desconocidas y para finalidades que igualmente ignoran. En consecuencia, el tratamiento de datos personales ha de incluirse entre los fenómenos que forman parte del "liberties pollution" o contaminación de libertades, es decir, ante la situación de *"erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías"*[1]. El uso desviado de la tecnología de tratamiento de datos personales supone además claros peligros para la libertad y para los derechos a no ser discriminado y a la propia dignidad e identidad personal.

2. Esta nueva forma de amenaza para los derechos y libertades de las personas ha originado el nacimiento de un nuevo derecho fundamental que dota al individuo de un poder de control sobre la información que le concierne: el derecho fundamental a la protección de datos personales. Este derecho se encuentra recogido en el apartado 4 del artículo 18 del texto constitucional que dispone lo siguiente: *"la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Si bien dicho precepto ha sido la respuesta del constituyente a una nueva forma de amenaza contra la dignidad de la

[1] PÉREZ LUÑO, A. E.: "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Corpus Data", en GARCÍA SAN MIGUEL, L.: *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992, p. 37.

persona y los derechos fundamentales, su inclusión dentro del mismo precepto constitucional que garantiza el honor, la intimidad personal y familiar y la propia imagen, la ausencia de un precepto constitucional íntegro, tal y como sucede en el artículo 35 del texto constitucional portugués en el que parece tener su origen el inciso final del artículo 18, y la previsión constitucional de acceso a los archivos y registros públicos, contenida en el artículo 105.b del texto constitucional, de forma independiente y con unas garantías menores a las previstas para el artículo 18, ha provocado en el pasado discrepancias en cuanto a su interpretación[2].

3. El Tribunal Constitucional ha jugado un papel esencial en al consolidación del derecho a la autodeterminación informativa. En su sentencia 292/2000, de 30 de noviembre, concluye que, mientras el artículo 18.1 CE tiene como función proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno, el derecho fundamental a la protección de datos *"persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*. Este derecho da respuesta, en la nueva realidad derivada del proceso tecnológico, *"a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona"*: la libertad informática. Así, el objeto de protección del derecho a la protección de datos personales se extenderá *"a cualquier tipo de dato personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo los datos de carácter personal"*. Por tanto, esta protección se extenderá también a los datos públicos que, aún siendo accesibles al conocimiento de cualquiera, *"no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos"*. Es decir, los datos amparados son todos aquéllos que identifiquen o permitan la identificación de una persona.

---

[2] A pesar las discrepancias doctrinales surgidas en torno a este precepto, no puede obviarse, sin embargo, el acierto y la importancia de su inclusión en el texto constitucional en una etapa en la cual el objetivo último era construir *"un sistema jurídico-político que pudiese gestionar mejor de lo que se estaba haciendo hasta ese momento los problemas sociales y que sometiese los asuntos humanos al imperio de una ley respetuosa de los derechos humanos y las libertades fundamentales"*. PECES-BARBA MARTÍNEZ, G. y RAMIRO AVILÉS, M.A.: *"La Constitución. 25 años después"*, en PECES-BARBA MARTÍNEZ, G. y RAMIRO AVILÉS, M.A.: *La Constitución a examen. Un estudio académico 25 años después*, Universidad Carlos III de Madrid- Instituto de Derechos Humanos "Bartolomé de las Casas", Marcial Pons, Madrid, 2004, p. 13.

4. El derecho fundamental a la protección de datos personales se constituye como un derecho instrumental para la garantía de otros derechos, constitucionales o no. El artículo 18.4 CE hace mención expresa a dos derechos fundamentales que podrían verse amenazados por un uso abusivo e ilegítimo de las nuevas tecnologías de la información: los derechos al honor y a la intimidad personal y familiar de los ciudadanos. No obstante, otros derechos podrían resultar afectados: el derecho a no ser discriminado, la libertad ideológica o religiosa, la presunción de inocencia, etc.

5. El contenido del derecho a la protección de datos personales se recoge en diversas normas sobre esta materia. En el plano estatal, el desarrollo legislativo general del artículo 18.4 CE se produce a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPDP) que ha sido objeto de desarrollo por el Real Decreto 1720/2007, de 21 de diciembre. Asimismo, el derecho ha tenido su reconocimiento y desarrollo en el ámbito internacional y comunitario. Entre la normativa de desarrollo se pueden citar, por su especial relevancia, el Convenio 108 del Consejo Europeo, de 28 de enero de 1981, para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y la Directiva 95/46/CE del Parlamento y del Consejo de la Unión Europea, de 24 de octubre de 1995, sobre Protección de las personas en lo que respecta al Tratamiento de Datos Personales. Interés particular reviste su reconocimiento en el artículo 8 de la Carta Europea de Derechos humanos como derecho autónomo[3]: *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. 3. El respeto de esta normas quedará sujeto al control de una autoridad independiente"*. Recogido en estos términos, la Carta no sólo proclama su existencia, sino que le atribuye un contenido concreto.

[3] Sobre la oportunidad de su reconocimiento en el citado texto, Vid. Dictamen 4/1999, aprobado el 7 de septiembre de 1999 por el Grupo de Trabajo sobre la protección de las personas física en lo que respecta al tratamiento de datos personales, relativo a la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales.

6. La Ley Orgánica 15/1999 intenta identificar los riesgos que para los derechos de las personas suponen el tratamiento de sus datos personales y al mismo tiempo garantizar los intereses legítimos, públicos o privados que justifiquen ese tratamiento. Así, establece, en su artículo 4, los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales de tal modo que sólo tendrán una calidad adecuada aquéllos respecto de los cuales se cumplan estos principios. En definitiva, se trata de normas que regulan la recogida, registro y uso de los datos personales y están encaminadas a garantizar tanto la veracidad de la información contenida en los mismos como la congruencia y racionalidad de su utilización.

Estos principios de calidad de los datos son los siguientes: en primer lugar, el principio de pertinencia que exige que los datos personales estén relacionados con el fin perseguido por lo que deberán ser *"adecuados y no excederán de las finalidades para las que se hayan registrado"*[4] (artículo 4.1 LOPDP). En segundo lugar, el principio de finalidad implica que sólo se podrán recoger y tratar automáticamente los datos personales que "sean adecuados (…) en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Además, los datos personales objeto de tratamiento "no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" (artículo 4, apartados 1 y 2 LOPDP). El principio de finalidad garantiza a los ciudadanos la posibilidad de controlar el uso de sus datos personales, "ofreciéndole una respuesta precisa y concreta a la cuestión de para qué van a ser utilizados, impidiendo además usos diferentes o incompatibles con el consentido"[5]. Por otra parte, el principio de veracidad y de exactitud supone la necesidad de que los datos sean "exactos y puestos al día de forma que respondan con veracidad a la situación del afectado" (artículo 4.3 LOPDP). El principio de lealtad, significa que los datos personales han de obtenerse sin engaños o falsedades por parte de quien los solicita, prohibiéndose de forma contundente la utilización de medios fraudulentos, desleales o ilícitos (artículo 4.7 LOPDP). Finalmente, el principio de seguridad de los datos supone la obligación de que se

[4] PÉREZ LUÑO, A. E.: "Los derechos humanos en la sociedad tecnológica", en LOSANO, M. y otros: *Libertad informática y leyes de protección de datos*, Centro de Estudios Constitucionales, Madrid, 1990, p. 166.

[5] GARRIGA DOMÍNGUEZ, A.: "La sociedad transparente o vulnerable", en *Efectos de las tecnologías de la información sobre los derechos humanos*, Institut de Drest Humans de Catalunya, Barcelona 2010, p. 92.

adopten las medidas necesarias para garantizar la seguridad de los datos personales evitando su alteración, pérdida, tratamiento o acceso no autorizados.El incumplimiento de cualquiera de estos principios supone la ilicitud del tratamiento de los datos que será potencialmente lesivo para los derechos de las personas.

7. Con la finalidad de evitar que los principios de calidad de los datos queden vacíos de contenido y el titular de los datos desamparado ante su tratamiento, el poder de disposición de los propios datos se llevará a cabo mediante un conjunto de facultades que forman el contenido del conocido como "habeas data"[6] y que *"consistirán en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos"*[7]. Esta facultades son las siguientes: el primer lugar, el derecho de información implica el derecho del titular de los datos a que se le informe de los bancos de datos existentes, de su titularidad y de su finalidad y de los derechos que le asisten. El artículo 5 LOPDP establece que las personas de las que se soliciten informaciones personales deberán ser informadas, de manera previa a la recogida de los mismos y de modo expreso, preciso e inequívoco, sobre la existencia de un fichero o tratamiento de datos personales, la finalidad de su recogida y los destinatarios de la información, el carácter obligatorio o facultativo de las respuestas a las cuestiones planteadas; las consecuencias de la obtención de los datos o de la negativa a facilitarlos; la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y la identidad y dirección del responsable del tratamiento o de su representante. Asimismo, establece este precepto, en su apartado 5, la obligatoriedad de informar a los interesados cuando los datos no hayan sido recabados directamente de ellos en los términos y sobre las cuestiones anteriores. En segundo lugar, el derecho del interesado a que se solicite su consentimiento inequívoco para la recogida, tratamiento y cesión de sus datos personales (artículo 6 LOPDP). Por otra parte, el derecho a una protección especial de los denominados datos sensibles que son informaciones relativas a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana (artículo 7 LOPDP). En cuarto lugar, el derecho de acceso de los afectados a las informaciones que les conciernen y las facultades de rectificación y cancelación de los

[6] Vid. SSTC 254/1993, de 20 de julio; 11/1998, de 13 de enero; 94/1998, de 4 de mayo y 202/1999, de 8 de noviembre.
[7] STC 292/2000, de 30 de noviembre.

datos personales que constituyen un instrumento idóneo para el control por los ciudadanos de la información sobre ellos registrada por entidades públicas o privadas ya que, en el ejercicio de estos derechos, el interesado podrá conocer quién y para qué tiene sus datos, corregir los incorrectos y cancelar los que no debían haber sido registrados o los que ya han cumplido su finalidad. Finalmente, el derecho al olvido que implica la cancelación de los datos personales, de oficio o a instancia del interesado, una vez transcurrido un determinado período de tiempo, lo cual supone la cancelación de los datos que ya no son necesarios de conformidad con el principio de finalidad (artículo 4.4, 5 y 6 LOPDP).

8. El derecho al olvido contrarresta uno de los riesgos más característicos del procesamiento informático de la información personal: *"la posibilidad de recuperar en un instante cualquier dato por insignificante que éste parezca, aun habiendo transcurrido decenas de años, lo que significa la desaparición de la garantía que suponía para la privacidad de las personas la fragilidad de la memoria humana"*[8].

9. Cuando la información de carácter personal se halla publicada en Internet, se complica la operatividad de las normas nacionales e internacionales que establecen los requisitos a respetar por aquéllos que pretenden recoger, tratar, utilizar o comunicar a terceros información sobre personas. La razón de esta complejidad radica en la dificultad que, en determinados casos, plantea la cancelación de dicha información y el control de sus usos y destinos. En consecuencia, para evitar esta falta de control, resulta imprescindible un uso cauto y responsable de las TIC, sobre todo en relación con colectivos especialmente vulnerables como es el caso de los menores de edad.

10. En el ámbito de las redes sociales, resulta conveniente que los usuarios de las mismas seleccionen detenidamente los datos que van a publicar, siendo respetuosos con la privacidad de otras personas y absteniéndose de publicar información sobre ellas sin su consentimiento. Asimismo, los proveedores de estos servicios, deben cumplir estrictamente la normativa sobre protección de datos personales además de adoptar las medidas necesarias para informar al usuario sobre el tratamiento de sus datos y las posibles consecuencias y riesgos de la publicación de informaciones personales y

[8] GARRIGA DOMÍNGUEZ, A.: "La sociedad transparente o vulnerable", ob. cit., p. 94.

permitiendo el control por parte de dichos usuarios sobre el uso secundario de perfiles y datos de tráfico y mejorando la seguridad de sus sistemas.