ESTUDIOS

LA PROTECCIÓN DE DATOS PERSONALES EN INTERNET

MARÍA DE LOS REYES CORRIPIO GIL-DELGADO (*)
Profesora de la Universidad Pontificia Comillas de Madrid

SUMARIO : Introducción.—1. Fuentes del sistema de protección de datos personales. 1.1 Regulación. 1.2 Autorregulación.—2. Contenido de la protección de datos personales. 2.1 En general. 2.2 En Internet.—3. Los tratamientos invisibles. 3.1 El deber de información 3.2 Finalidades leales. 3.3 El principio del consentimiento.—4. Los nuevos derechos de la protección de datos personales en Internet. 4.1 El derecho a realizar opciones informadas. 4.2 El derecho al anonimato. 4.3 El derecho a utilizar herramientas de seguridad en la red.—5. Conclusiones.

Introducción

Internet constituye un entorno tecnológico y social nuevo que genera riesgos para la vida privada de las personas que navegan o cuyos datos circulan por la red. Su especial fisonomía viene en gran medida marcada por la interactividad de las comunicaciones y la generación de un elevado número de datos transaccionales o de conexión permanentes y utilizables para finalidades diversas. La problemática procede de que los datos de navegación del usuario conservados por el proveedor de acceso (datos de conexión asociados a la dirección IP) pueden permitir un seguimiento de la actividad de un internauta (los webs visitados, la fecha y la hora, los documentos telecargados, la participación en un espacio de discusión, los mensajes electrónicos enviados o recibidos) durante todo el tiempo en que se conserven estos datos.

Para abordar esta problemática comenzaremos por las fuentes del sistema de protección de datos personales para, a continuación, estudiar los principios y derechos aplicables a los tratamientos realizados en Internet.

(*) Autora del libro «Regulación jurídica de los tratamientos de datos personales realizados por el Sector Privado en Internet», galardonado con el Premio «Protección de Datos Personales», IV edición, 2000, otorgado por la Agencia de Protección de Datos.

1. Fuentes del sistema de protección de datos personales

Las fuentes de donde extraemos el régimen jurídico de protección de los datos de carácter personal están constituidas, por un lado, por las normas que lo regulan y por otro, con diverso alcance, los sistemas de autorregulación.

1.1 Regulación

En nuestro país la regulación de la protección de datos personales comenzó con la inclusión en nuestro texto constitucional del artículo 18.4, por el cual *«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»*. Posteriormente la ratificación del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 [1], dio un cierto contenido al artículo 18.4 de la Constitución Española pendiente aún de desarrollo legislativo.

Con la adopción de la Ley Orgánica 5/1992, 29 de octubre de Regulación del Tratamiento automatizado de los datos de carácter personal (LORTAD), se articuló todo un sistema legal de protección basado en tres factores: sujeción de todo tratamiento de datos a unos principios de legitimidad, reconocimiento de un haz de derechos y creación de instituciones jurídicas, dirigidas a tutelar la adecuación del marco de garantías.

La posterior aprobación de la Directiva 95/46/CE [2] (Directiva general) llevó a la necesidad de introducir modificaciones en la LORTAD, y se optó por aprobar una nueva Ley Orgánica, 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) [3]. En ella se recogen nuevos derechos como el de oposición al tratamiento, y se dan solución a los problemas suscitados en la aplicación de la LORTAD, por ejemplo el caso de los tratamientos de datos del censo.

Aunque esta normativa general se aplica a los tratamientos de datos personales en Internet, la Comisión Europea ha aprobado una Directiva específica dirigida a proteger los derechos de las personas, en particular el de la intimidad, ante los tratamientos de datos personales realizados en las redes públicas digitales. Nos referimos a la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones [4], que reconoce entre los derechos específicos de este sector: el deber de informar de la falta de seguridad, el derecho a la destrucción de los

---

[1] Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Hecho en Estrasburgo, el 28 de enero de 1981 (BOE de 15 de noviembre de 1985). Vid en este sentido la Recomendación de la Comisión 81/679/CEE, de 29 de julio de 1981, relativa al convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (DOCE L 246, de 29 de agosto de 1981, p. 31).

[2] Directiva 95/46/CE del Parlamento y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE núm. L 281 de 23 de noviembre de 1995, p. 31 y ss.).

[3] La regulación de esta materia en nuestro país está contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), publicada en el «BOE» núm. 298, de 14 de diciembre de 1999.

[4] DOCE num. 24 de 30 de enero de 1998.

datos sobre el tráfico y la facturación, los derechos sobre la facturación, la identificación de las líneas de llamada y las guías de abonados [5].

Las disposiciones de esta norma están orientadas primordialmente a los tratamientos relacionados con la telefonía fija. De ahí el interés por adaptar esta normativa sectorial a los tratamientos realizados en Internet por medio de una nueva directiva del Parlamento europeo y del Consejo que sustituya a la Directiva 97/66/CE [6].

1.2 Autorregulación

Aunque no es exclusiva de este entorno, la autorregulación juega en Internet un papel importante, dado su gobierno anárquico, su carácter internacional y la dificultad de regular los comportamientos en la red mediante leyes o reglamentos convencionales. La particular fisonomía de Internet ha favorecido el empleo de sistemas de autorregulación, principalmente a través de dos instrumentos: los códigos de conducta y las políticas de privacidad de los sitios *Web*.

La Unión Europea admite la elaboración de códigos de conducta [7] creados en el marco de asociaciones y susceptibles de un mayor control por parte de los órganos de gobierno de la asociación. Estos han sido reconocidos como instrumentos válidos en la normativa comunitaria y su estructura y funcionalidad posee ya un respaldo legal [8].

Las empresas que tratan datos personales de los usuarios que navegan por Internet o de sus clientes que acceden on line, deben, a la hora de tratar los datos de estos, someterse a una política coherente y protectora de la vida privada denominada «política de privacidad» [9]. Los titulares de sitios *Web* y proveedores de servicios deben, en primer lugar, asegurar a los usuarios que el tratamiento que realizarán de sus datos personales será leal y lícito, indicando las finalidades para las que dichos datos son recogidos y tratados así como las medidas de seguridad de los sistemas informáticos que emplean, y asegurar a los usuarios la confidencialidad de la información en el sentido de establecer controles rigurosos para el acceso a los datos personales. Deben, en segundo lugar, darle a los usuarios la oportunidad de optar a que sus datos no sean tra-

---

[5] Para más información sobre este tema, *vid.* R. Corripio Gil-Delgado, C. Fernández Aller, *La protección de los datos personales en las autopistas de la información,* Aranzadi, Volumen «XII Encuentro sobre Informática y Derecho», Pamplona 1999, pp. 105 y ss.

[6] Propuesta de directiva del Parlamento europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (500PC0385).

[7] *Vid* artículo 27 de la Directiva General, por el cual se dispone que los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes, puedan someterlos a examen de las autoridades nacionales.

[8] El artículo 32 LOPD admite el recurso a los códigos tipo como medio de regular los derechos, obligaciones, medidas de seguridad, modalidades de ejercicio, etc., de los responsables de tratamientos de datos personales: «1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupan, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo».

[9] *Vid. http://www.privacyalliance.org/resources/ppguidelines.shtml*

tados o destinados a determinadas finalidades, como por ejemplo prospección comercial.

Estas mismas exigencias vienen contempladas en la Recomendación R (99) 5 del Consejo de Europa sobre la protección de las personas en relación con la colecta y el tratamiento de datos de carácter personal en las autopistas de la información.

En particular si se tratan datos personales de menores, las políticas de privacidad deben hacer referencia a ellos como la instauración de sistemas de información efectivos o la obligación de obtener el consentimiento de los padres antes de tratar los datos personales de sus hijos o, incluso, permitirles a éstos revisar la información personal recopilada sobre ellos, revocar su consentimiento y borrar la información colectada de sus hijos a solicitud paterna.

Para cumplir con el deber de información exigido por la normativa nacional y comunitaria los titulares de sitios *Web* deberían fijar en una nota informativa *(«privacy notices»)* y en la primera página a la que accede el visitante *(«Homepage)* información relativa a su política de «privacidad», mediante la instalación de vínculos a páginas que recojan el contenido de dicha política [10].

La importancia de la autorregulación en Internet es grande, si bien desde un punto de vista jurídico, mayormente desde nuestra perspectiva continental, parecen soluciones ubicadas más en el ámbito de la ética y buenas maneras que en el campo del derecho, en cuyo caso obligarían moral y no jurídicamente. Estas normas podrían carecer de la correspondiente acción quedando fuera del ámbito del derecho subjetivo.

Nos encontramos ante la tradicional controversia entre el deber natural y el deber jurídico y aunque estimamos que no es éste el lugar adecuado para analizar exhaustivamente la naturaleza jurídica de la autorregulación, es preciso realizar dos consideraciones: si, en general, las normas de autorregulación son deberes naturales y no jurídicos, entrañan «obligaciones imperfectas» de las que «no somos responsables sino ante Dios, y que no dan a persona alguna derecho de exigir su cumplimiento» [11]; un término medio entre la obligación civil y el acto de liberalidad [12]. Por otra parte, la autorregulación puede relacionarse jurídicamente con conceptos como la buena fe y el *neminem ledere,* de forma que si su incumplimiento procede de la mala fe de un tercero o produce un daño a una persona, ésta se encuentra revestida de un derecho subjetivo a reclamar. Por último, podemos considerar que su exigibilidad jurídica procede de su consideración como *uso social,* como costumbre, y que la autorregulación sea una forma de generación de costumbre en la nueva sociedad que se está gestando.

2. Contenido del sistema de protección de datos personales

En materia de contenido, el sistema legal de protección de datos personales ha ido evolucionando en los últimos años. La creación de bases de datos más elaboradas que, a diferencia de las tradicionales, recopilan datos relacionados con los gustos, prefe-

---

[10] *http://www.arnal.es/free/noticias/free2_17.html#T4*

[11] POTHIER, R.J. «Tratado de las Obligaciones». Heliasta. 1979, artículo preliminar.

[12] COLIN; CAPITANT. «Curso elemental de Derecho civil». RGLJ. Ed. Reus, Tomo III. Madrid 1960, p. 109.

rencias, comportamiento, etc. de clientes y usuarios, ofrece nuevos riesgos y favorecen la aplicación de técnicas conocidas como el *datawharehouse o data minnius,* utilizadas para segmentar la clientela.

No se trata sólo de la elaboración de bancos de datos relativos al comportamiento de las personas, sino el tratamiento posterior que se hace de ellos, como su transferencia a terceros o su utilización para el mercadeo de productos no solicitados. La tecnología digital permite aplicar técnicas de publicidad *one to one* mucho más agresivas y baratas que los tradicionales medios de comunicación como el teléfono o la correspondencia.

2.1 En general

La normativa ha ido evolucionando y acogiendo nuevos principios y excepciones. Así, la Directiva europea 95/46/CE, de protección de datos personales (Directiva general) [13], que recoge casi textualmente los principios del Convenio 108 del Consejo de Europa sobre calidad de los datos (artículo 6 de la Directiva general [14]), incorpora otros relativos a la legitimación del tratamiento de datos (artículo 7 de la Directiva general) referidos básicamente a la necesidad de consentimiento del interesado (letra a) o a otros supuestos de licitud del tratamiento no basada en dicho consentimiento (letras b) a f), o al derecho de oposición (artículo 14 de la Directiva general).

Junto al principio del consentimiento se potencia y precisa en gran manera el deber de información que había sido recogido como garantía complementaria en el artículo 8 a) del Convenio [15], introduciendo (artículos 10 y 11 de la Directiva general) deberes específicos para el responsable del tratamiento o su representante, de comunicar ciertas informaciones al interesado. También se introducen garantías explícitas frente al tratamiento de datos con fines de prospección *(vid* artículo 14 b de la Directiva general) y matizaciones relacionadas con la seguridad del tratamiento, añadiéndose deberes de confidencialidad (artículo 16 de la Directiva general) y la obligación del responsable de adoptar medidas de seguridad y organización adecuadas (artículo 17 de la Directiva general).

En esta línea de evolución del sistema legal de protección de datos personales deben acogerse nuevos derechos y adaptarse las disposiciones a las peculiaridades que suscitan los nuevos medios, en particular Internet. El crecimiento de la información colectada a través de Internet aumenta las preocupaciones referidas a la información personal que puede ser recolectada a distancia sin el consentimiento del usuario y a la seguridad del almacenamiento y transferencia de la información.

---

[13] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE núm. L 281 de 23 de noviembre de 1995, p. 31 y ss). Desde mucho antes, la protección frente al tratamiento de datos personales ha sido objeto de preocupación por la Comunidad Europea. El Parlamento europeo había manifestado en una serie de resoluciones, su inquietud sobre esta cuestión *(vid.* DOCE C 100 de 3 de mayo de 1976, p. 27, DOCE C 140 de 5 de junio de 1979, p. 34 y DOCE C 87 de 5 de abril de 1982, p. 39) e invitado a la Comisión a preparar una propuesta de directiva de armonización de las legislaciones en materia de protección de datos personales.

[14] Según este principio, los datos serán tratados de manera leal y lícita, recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Deberán ser adecuados, pertinentes y no excesivos, exactos y actualizados y conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

[15] «Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero».

Al aplicar el sistema de protección de datos existente al contexto de Internet „algunos principios, como el derecho de información, el principio del consentimiento o el deber de seguridad, adquieren relevancia particular. Éste último constituye uno de los principios más sobresalientes en Internet, dado su carácter abierto, en particular en servicios como las páginas *Web*, que, a diferencia de otros, no son muy favorables a impedir el acceso a la información de una persona determinada [16].

2.2 En Internet

La protección de datos personales en Internet pasa necesariamente por el fortalecimiento de los sistemas de control en la fase de recogida de datos, pues, una vez colectados éstos, quedan fuera del entorno de poder del usuario y del marco jurídico de protección arbitrado por el país de origen.

En el sistema de protección de datos personales existe, además, un principio de limitación en materia de colecta, de forma que todo dato de carácter personal identificado o identificable deberá ser recogido de forma leal y lícita y, en su caso, mediando el consentimiento el afectado [17]. A la recogida leal se añaden la sujeción de la colecta a fines determinados, explícitos y legítimos [18] (finalidades que deberán ser determinadas a más tardar en el momento de realizar la colecta [19]) y el principio de calidad de los datos.

Este marco jurídico viene igualmente recogido en el artículo 5 LOPD a través del cual el legislador exige la lealtad en la recogida de datos. Atendiendo a la normativa podemos establecer un distinto régimen jurídico según se trate de datos recogidos del propio interesado, de fuentes accesibles al público o bien de otras fuentes. Un ejemplo de estos últimos son los datos relacionados con la navegación de los usuarios (datos transaccionales y archivos persistentes) y que por ser ocultos al a éste han recibido el nombre de «tratamientos invisibles» [20].

En el supuesto de datos recabados del propio interesado, podríamos pensar que la entrega por parte de éste (consentimiento) da legitimidad a la recogida. Sin embargo, resultan habituales ciertas prácticas, como la oferta de servicios gratuitos orientados a recabar datos de navegantes y usuarios, que comprometen así su vida privada [21], o la obligatoriedad para los visitantes de una página *Web* de rellenar cuestionarios sin que los titulares de las mismas hayan precisado las finalidades a que se van a destinar las informaciones recopiladas de sus visitantes. En la mayoría de los casos se trata de formularios que el internauta debe rellenar inscribiendo la dirección electrónica, la identidad, las referencias postales o telefónicas así como las informaciones socioeco-

---

16 Gringras, C. De Nabarro Nathanson. The Laws of the Internet. Butterworths. London, 1997, p. 249.

17 Vid ad supra y además: The OECD privacy policy statement generator. Paris. *http://www.oecd.org/dsti/sti/it/secur/prod/generator-f.pdf*

18 Art. 6 de la Directiva 95/46/CE

19 *Vid.* Líneas Directrices de privacidad. OECD. 1980.

20 Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware,* aprobada el 23 de febrero de 1999: WP17 (5093/98).

21 «Cuando se responde en Internet a una oferta de información, productos o servicios gratuitos, y se suministran datos personales (incluyendo el propio interés en el tema en cuestión) se está poniendo en compromiso la privacidad de forma gratuita. Es necesario discernir quién tiene una necesidad legítima de disponer de los datos personales y quien no» (RIOS AGUILAR, S.; DIEZ PLATAS, M.L. «Problemas de Seguridad en la sociedad de la información». Libro de Actas. JIS'98, Segundas Jornadas Informática y Sociedad 1998. Ed. Departamento de Lenguajes y Sistemas Informáticos e Ingeniería de Software, Madrid, p. 349).

nómicas (profesión, ingresos...). Estas colectas suscitan serias dudas en relación con los principios de finalidad y calidad de los datos y consentimiento del interesado, establecidos por la normativa sobre protección de datos personales.

3 Los tratamientos invisibles en Internet

El supuesto de los tratamientos invisibles plantea mayores problemas, pues en la medida en que el tratamiento de los datos de conexión se realiza de forma invisible para el usuario, éste se ve privado de la posibilidad siquiera de ejercitar sus derechos. Los tratamientos invisibles son prácticas frecuentes no exentas de riesgos para la persona, ya que esos datos se emplean para múltiples finalidades, como elaboración de perfiles de comportamiento, estadísticas, cesión a otras compañías etc. Por ello hemos creído conveniente comenzar este apartado por el análisis de los principios que deben regir la recogida de los datos en Internet y de las finalidades que justifican una utilización más allá del fin para el que fueron recopilados.

Por todo ello, los actores de tratamientos invisibles deberán necesariamente cumplir tres principios básicos: el deber de información, el de adecuación a finalidades leales, y el principio del consentimiento.

3.1 El deber de información

Las personas deben ser informadas sobre la finalidad del tratamiento de estos datos y de sus derechos a oponerse al registro de ciertas categorías de servicios consultados, en concreto los que son susceptibles de mostrar el perfil del consumidor potencial, sus hábitos, sus opiniones políticas o religiosas, que constituyen además datos sensibles.

En el caso de las *cookies,* los mismos programas de navegación deberían informar a los usuarios por medio de un lenguaje comprensible, cuando está previsto su recepción, almacenamiento o envío y qué datos se pretende almacenar en el *cookie* así como el periodo de validez del mismo [22]:

No basta, pues, con indicar que se generará una *cookie* o que los datos serán conservados con fines de promoción comercial. Será también preciso que el usuario tenga noticia clara de [23]:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento a que van a ser objeto los datos;
c) cualquier otra información tal como:

— las categorías de los datos de que se trate,
— los destinatarios o las categorías de destinatarios de los datos,
— la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que

---

[22] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware.*, o.c., 5093/98/ES/final WP 17.
[23] Aplicación del artículo 11 de la Directiva general.

se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

El Informe del Consejo de Estado francés [24] sobre Internet y redes digitales manifiesta, sin embargo, que este enfoque no agota el tema en la medida en que principalmente algunos proveedores de acceso ofrecen un acceso gratuito a Internet o a un servicio de mensajería electrónico a cambio de la autorización del internauta para analizar con fines de prospección personal los datos de conexión que se relacionan con su « navegación « en Internet; esta práctica manifiesta fácilmente los límites que descansan en la elección individual de la persona.

3.2 Finalidades leales

El deber de información se extiende a las finalidades del tratamiento. En este sentido el artículo 4.1 LOPD recoge en su nueva redacción los adjetivos «determinadas, explícitas y legítimas», lo que refuerza la necesidad de una manifestación expresa y externa de las finalidades y, como consecuencia, un conocimiento por parte del afectado de que sus datos van a ser utilizados para otras finalidades. Además, el software navegador debería estar configurado, por defecto, de tal forma que sólo pudiera tratarse la mínima cantidad de información necesaria para establecer una conexión Internet [25].

Sobre los conceptos de «finalidad legítima» y proporcionalidad (artículo 5 de la convención 108 del Consejo de Europa recogido en la Directiva general) aplicados a los datos de conexión, existen algunos pronunciamientos, como la doctrina francesa de la CNIL que considera como tales la seguridad, a fin de evitar las penetraciones fraudulentas en el *Web* y la elaboración de estadísticas agregadas sobre las consultaciones del *Web*. Otras finalidades admitidas por la CNIL serían los fines estadísticos. En este sentido los archivos de *logs* podrían ser utilizados lícitamente para elaborar estadísticas agregadas.

También se pueden utilizar los archivos de datos transaccionales para medir la audiencia y fijar los precios del alquiler de banderas publicitarias en un determinado servidor. Las empresas se ven obligadas a recurrir a estos útiles, sobre todo teniendo en cuenta que la arquitectura particular del tipo cliente/servidor de la red Internet y el hecho de que los usuarios no están conectados permanentemente a un servidor, los hacen necesarios para determinar la dinámica real de las transacciones realizadas en el curso de una sesión [26]. Esta finalidad sería legítima siempre y cuando, principio de proporcionalidad, se aplicaran procedimientos de disociación sobre estos datos. En particular nos resultan útiles las reglas y principios contenidos en las disposiciones comunitarias sobre protección de datos con fines estadísticos.

---

[24] Consejo de Estado Francés. Estudios. De 8 de septiembre de 1998 Internet y las redes digitales.. *http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm*

[25] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware.*, o.c., 5093/98/ES/final WP 17.

[26] Comisión Europea, Dirección General de mercado interior y servicios financieros. «Les services en ligne et la protection des données et de la vie privée» Vol I. Exposé de la situation générale. Comunidades Europeas. Bruselas, 1998. p. 25.

3.3 El principio del consentimiento

No debería ser posible el tratamiento invisible de los datos de navegación del usuario, como la inscripción de una información en el disco duro de su ordenador, sin que fuese advertido, sin que pudiese oponerse y sin que pudiese conocer de manera inteligible el contenido de la misma [27].

El consentimiento a los tratamientos invisibles debe ser expreso y arbitrado desde los propios programas de navegación. Los productos de Internet, tanto de *hardware* como de *software,* deberían permitir al interesado decidir libremente sobre el tratamiento de sus datos personales, ofreciéndole instrumentos de fácil manejo para filtrar la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados [28], como una realización práctica del derecho del usuario a realizar opciones informadas.

Finalmente los sitios comerciales de páginas *Web* que colecten datos personales identificables de consumidores *online* deberán cumplir con cuatro prácticas de información leal generalmente aceptadas [29]:

— Noticias o menciones. Deberán mencionar de forma clara sus prácticas relacionadas con la información personal que colectan, cómo la colectan, para qué la usan, cómo podrán los consumidores ejercitar sus derechos de opción, acceso y seguridad, si la revelan a otras entidades, o si otras entidades están recopilando datos a través del sitio.

— Opciones. Los *Websites* deberán ofrecer a los consumidores opciones relacionadas con el tratamiento de su información personal. Esta opción podrá ir acompañada de usos internos secundarios como *marketing* directo a consumidores o usos externos secundarios, como revelación de datos a otras entidades.

— Acceso. Los *Websites* deberán ofrecer a los consumidores de forma razonable acceso a la información que sobre ellos se ha recopilado, incluyendo la posibilidad de revisar dicha información y de corregir inexactitudes o borrarla.

— Seguridad. Los *Websites* deberán adoptar las medidas pertinentes para preservar la seguridad de la información que colectan de los consumidores.

Resulta cuanto menos chocante la libertad con que los agentes involucrados en el tratamiento de los datos personales tratan los datos obtenidos de las comunicaciones interactivas en Internet, sobre todo si lo comparamos con las limitaciones al tratamiento de los datos sobre el tráfico recogidas en la regulación sobre protección de datos en el sector de las telecomunicaciones. Ello se explica porque la navegacion por Internet, aunque se trate de una comunicación electrónica, no lleva incorporado un mensaje (no nos referimos al correo electrónico obviamente o a otros sistemas de transmisión de mensajes o comunicaciones por Internet); porque la prestación de servicios de información determina el nacimiento de una «relación especial» de los «sitios» con los navegantes (cuanto más si son sus clientes) y, por último, porque, en este caso, los titulares de páginas *Web* serían los destinatarios de las comunicaciones y no terceros que acceden a comunicaciones ajenas.

---

[27] Consejo de Estado Francés. Estudios. De 8 de septiembre de 1998. Internet y las redes digitales.. *http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm*

[28] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware.*, o.c., 5093/98/ES/final WP 17.

[29] *http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf*

Por todo ello, las limitaciones a los tratamientos invisibles y la recogida de datos por los titulares desde las páginas *Web* debe encontrarse en un sistema de protección de datos personales adaptado a las características de los tratamientos y a la peculiar fisonomía de Internet. Esta adaptación se encuentra en el reconocimiento de deberes específicos en la fase de recogida de los datos, en particular, el derecho a realizar opciones informadas, el derecho al anonimato y a la seguridad en la red.

4 Los nuevos derechos de la protección de datos personales en Internet

La salvaguarda de la propia vida privada se encuentra en el comportamiento y control que efectúa el usuario y, en Internet, pasa necesariamente por el derecho a realizar opciones informadas, de forma que cuando se recaban datos por el sector privado, el interesado pueda escoger libremente cuáles de sus datos quiere comunicar y para qué finalidades. Ligado a este derecho se encuentran el derecho al anonimato y a utilizar herramientas de seguridad

4.1 El derecho a realizar opciones informadas

La libertad informática otorga al interesado un derecho a controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un registro informático que le conciernen. Como indica LUCAS [30], el individuo puede definir la intensidad con que desea que se conozcan y circulen su identidad y circunstancias. Esta capacidad de decisión debe ocupar un papel fundamental en Internet, mediante el derecho a realizar «opciones informadas».

Ello es así porque no existe en el sector privado una obligación general de entregar ciertas categorías de datos, pues no hay una primacía de intereses entre los particulares, a diferencia de lo que puede ocurrir en el sector público. Por otra parte, una prohibición absoluta tampoco es recomendable, pues el usuario puede tener interés en comunicar sus datos, por ejemplo para obtener información o para celebrar determinados contratos, aunque, en muchas ocasiones, la práctica comercial, sobre todo para la realización de perfiles de usuarios, suele pedir al particular abundante información personal (como número de hijos, sector profesional, preferencias, etc.) sin informarle previamente de las finalidades del tratamiento.

No basta con asegurarle al usuario que se adoptarán las medidas técnicas adecuadas para impedir la destrucción accidental o el acceso no autorizado, es necesario también dotarle de herramientas para conocer y realizar opciones informadas cuando van a tratarse sus datos personales en algún servicio de Internet que le permitan decidir si cede o no sus datos.

El estándar *(OPS Open Profiling Standard)* permite a los internautas una mayor libertad de elección sobre el tipo de informaciones que desean divulgar y ofrece en todo momento la posibilidad de modificarlas. El objetivo de la Norma de Perfiles Abierta es garantizar la transmisión segura de un perfil normalizado de datos perso-

[30] Lucas Murillo de la Cueva, P. «El derecho a la autodeterminación informativa». Tecnos. Temas clave de la Constitución española, Madrid, 1990, p. 174.

nales a condición de que las «prácticas en materia de privacidad» informática declaradas por el sitio satisfagan las exigencias del usuario [31].

Por su parte, el Consorcio *World Wide Web* ha elaborado la Plataforma de Preferencias de Privacidad como medio para desarrollar un estándar dirigido a que los usuarios conozcan las prácticas relacionadas con el tratamiento de datos personales de los sitios Web *(privacy policy)* [32]. El objetivo de esta plataforma consiste en que el usuario presta su consentimiento para que un sitio Internet registre sus datos personales a condición de que las «prácticas de privacidad» declaradas por el sitio satisfagan las exigencias del usuario, sobre todo en relación al propósito para el cual se registran los datos, y si estos datos se utilizan o no para fines secundarios o se ceden a terceros. Esta herramienta opera comparando las «políticas de privacidad» del sitio con las preferencias expresadas por el usuario, ayudándole a decidir cuándo entregar datos personales en Sitios Web [33]. A diferencia de los sistemas de anonimato en la red que previenen contra la transferencia de información identificable, aquí se parte de la base de que los usuarios desean en ocasiones revelar información personal [34].

Sin embargo su implantación depende de la solución de diversos problemas [35] como por ejemplo la necesidad de introducir en los programas de navegación opciones «por defecto», «que reflejen el interés del usuario por disfrutar de un elevado nivel de protección (incluida la capacidad de navegar por los sitios de la Red de forma anónima) sin verse bloqueado o sufrir molestias por su intento de acceder a sitios».

El derecho a realizar opciones informadas debe complementarse ineludiblemente con el derecho al anonimato como opción básica del usuario que navega o contrata por la red.

4.2 El derecho al anonimato en Internet

Hay anonimato cuando la comunicación no deja traza electrónica. La creación de un marco de comunicaciones anónimas respetadas y fomentadas por la normativa surge como respuesta necesaria y preventiva a la vulnerabilidad y vigilancia en Internet.

Sobre la articulación jurídica del anonimato, cabría preguntarse si es posible su reconocimiento como contenido esencial del derecho a la protección de datos personales en Internet.

En realidad el anonimato en las comunicaciones ha estado vinculado a diversos derechos fundamentales como la libertad de expresión o el secreto de las comunica-

---

[31] Grupo de Trabajo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales (Grupo de trabajo del art. 29). Dictamen 1/1998. Plataforma de Preferencias de Privacidad y Norma de Perfiles Abierta (OPS), adoptada por el Grupo de Trabajo el 16 de junio de 1998.

[32] Para más información vid. http://www.w3.org/P3P/; y en cuanto artículos: VILLATE, J «P3P, un estándar para la privacidad ¿es lo que necesitamos?. Revista Electrónica de Derecho Informático, 1 de agosto de 1998, *http://publicaciones.derecho.org/redi/*No._01_-_Agosto_de_1998/villate.

[33] FAITH CRANOR, L. Agents of choice: tools that facilitate notice and choice about Web site data practices, 1999, *(http://www.research.att.com/*(...)lorrie/).

[34] FAITH CRANOR, L Agents of choice: tools that facilitate notice and choice about Web site data practices, 1999, *(http://www.research.att.com/*(...)lorrie/).

[35] Grupo de Trabajo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales (Grupo de trabajo del artículo 29). Dictámen 1/1998. Plataforma de Preferencias de Privacidad y Norma de Perfiles Abierta (OPS), adoptada por el Grupo de Trabajo el 16 dejunio de 1998.

ciones. El anonimato no sólo garantiza la intimidad sino que refuerza la libertad de expresión, pues los usuarios pueden participar libremente en la red sin temor a que sus rastros sean seguidos. En Estados Unidos el derecho a comunicarse de forma anónima está protegido por la Primera Enmienda y el poder hablar anónimamente ha jugado un importante papel a lo largo de la historia permitiendo a los individuos criticar prácticas opresoras y leyes que no hubieran sido de otra forma criticadas [36]. El anonimato de las comunicaciones forma parte también del derecho fundamental al secreto de las comunicaciones y del correlativo deber de confidencialidad. Este derecho prohibe cualquier forma de interceptación o vigilancia por quien no sea su remitente o su destinatario salvo que esté legalmente autorizada [37].

En el sistema de protección de datos personales existe también un cierto derecho al anonimato entre las disposiciones que regulan el sector de las telecomunicaciones o en sectores específicos como la investigación científica y estadística [38]. Nos centraremos en el primer supuesto porque es en definitiva en las comunicaciones electrónicas donde el anonimato juega un papel fundamental.

En la práctica, el anonimato frente a los operadores es posible en los servicios de telefonía gracias a la existencia de cabinas públicas que impiden la identificación del originador de la llamada por el propio operador. Podríamos, por tanto, pensar que el derecho al anonimato debe reconocerse también frente a los operadores, algo que tecnológicamente es posible.

Por último, aunque lo reconozcamos como un derecho, y tal reconocimiento sea particularmente interesante en Internet, no por ello afirmamos que se trata de un derecho absoluto. El anonimato también presenta problemas legales pues permite ocultar la identidad en la red de los que cometen delitos por este medio. La defensa nacional, el interés público,o la prevención del blanqueo de capitales y otros bienes jurídicos entran en juego a la hora de permitir el anonimato en Internet. El derecho a comunicarse anónimamente, protegido por la libertad de expresión, el secreto de las comunicaciones y la vida privada, tienen también sus límites y está sujeto a controles gubernamentales. De ahí la prohibición inicial de anonimato en las comunicaciones y del envío de información cifrada en los orígenes de las comunicaciones [39], y las limitaciones a exportación de productos de cifrado (considerado material de doble uso).

4.3 El derecho a utilizar herramientas de seguridad de la red

Cuando a pesar de las medidas de seguridad aplicadas, subsista un riesgo concreto de violación de la seguridad de la red, el prestador de un servicio de telecomunicación

---

[36] Smedinghoff, T.J. «Right of Privacy». Vol. Online Law. Ed. Software Publishers Association, Massachusetts 1996.

[37] *Vid* artículo 5.1 Directiva 97/66/CE, de protección de datos personales en el sector de las telecomunicaciones (aunque esta normativa deriva de la regulación del secreto de las comunicaciones).

[38] La Recomendación R (83) 10 del Consejo de Europa de 23 de septiembre de 1983 (publicado en Estrasburgo en 1984), sobre protección de los datos de carácter personal con fines de investigación científica y de estadística, reconoce que para que el respeto a la vida privada quede garantizado, la investigación debe, en la medida de lo posible, utilizar datos anónimos. Las organizaciones científicas y profesionales así como las autoridades públicas deben promover el desarrollo de técnicas y procedimientos que aseguren el anonimato. El derecho de la persona a obtener y rectificar los datos que le conciernen puede quedar restringido cuando los datos hayan sido recabados y retenidos con fines puramente estadísticos o de otras investigaciones. Sobre esta misma materia *vid* también la Recomendación R (97) 18, relativa a la protección de datos personales recopilados y tratados con fines estadísticos, adoptada el 30 de septiembre de 1997.

[39] Smedinghoff, T.J. «Right of Privacy». Vol. Online Law. Ed. Software Publishers Association, Massachusetts, 1996.

tendrá la obligación suplementaria de informar a las personas sobre la existencia de dicho riesgo y sobre las posibles soluciones, incluidos los costes necesarios [40].

La percepción por el usuario de que la red es insegura, le permitirá escoger un dispositivo eficaz para preservar la seguridad de las informaciones personales que envía por Internet. Entre estos dispositivos incluimos el uso de claves y contraseñas, cortafuegos y el uso del cifrado.

La utilización de palabras clave para establecer la autenticidad del usuario de la tarjeta magnética conocidas sólo por el cliente y por el banco es el método tradicional de autenticación, por ejemplo de una tarjeta magnética. Para ello se introducen en el ordenador un par de parámetros, denominados número o código de identificación del usuario y contraseña o *password* [41]. Estos procedimientos de contraseñas y claves resultan franqueables e insuficientes para garantizar el acceso no autorizado a determinados sistemas informáticos.

El «cortafuegos» o *firewall* se puede definir como «un sistema o conjunto de éstos cuyo objetivo es hacer cumplir una política de control de acceso entre dos redes, una de las cuales es, en muchos casos, Internet» [42]. El *firewall* es un dispositivo físico que controla las entradas al servidor para que sólo se pueda entrar por los puertos preestablecidos; se introducen en esta máquina unas reglas de filtración mediante la comprobación del correo entrante y saliente. Por ejemplo, es posible configurar un cortafuegos solamente para permitir la comunicación con páginas específicas [43]. El cortafuegos incorpora un *software* dirigido a supervisar el tráfico para comprobar si el propósito de la comunicación es legítimo. Las pruebas incluyen el origen o el destino de los datos o el contenido del mensaje. El examen del origen y destino de un mensaje puede impedir que el personal de una empresa acceda a ubicaciones no deseables (p.ej. servidores de pornografía en Internet) o envío de información con fines no empresariales (p.ej. grupos de noticias de entretenimiento).

El cifrado del mensaje constituye una garantía para la seguridad de las comunicaciones. Su realización práctica en Internet se realiza mediante el empleo de algoritmos de cifrado que permiten transformar un mensaje escrito en claro, en un mensaje cifrado denominado criptograma. Este resultado es obtenido por medio de una transformación de la señal utilizando una o varias claves. Entre los medios tecnológicos orientados a la seguridad, destacan los siguientes: medios lógicos que aseguran la gestión de las claves privadas, firma digital, encriptación, autorización de acceso etc.; medios físicos, utilizando *smart cards* o sistemas informáticos asociados a otros dispositivos; medios mixtos, que permiten crear conjuntos sofisticados (cortafuegos), medios criptográficos [44].

---

[40] Artículo 4.2 Directiva 97/66/CE.

[41] El primero es un código que asigna el administrador del sistema a cada usuario, pero en ocasiones un ID puede ser asignado a un grupo de usuarios. Cuando un usuario se conecta al ordenador, éste le pide, en primer lugar, el ID, es decir procede a su identificación y posteriormente le solicita la contraseña (DÁVILA MURO, J.; MORANT RAMÓN, J.L.; SANCHO RODRÍGUEZ, J. «Seguridad lógica y física en los medios de pago electrónicos». Revista ICADE, núm. 43, 1998. p. 115).

[42] CAP GEMINI, Factbook Tecnologías de la Información, 2000 o.c., p. 535.

[43] El examen de las páginas implicadas en una interacción se puede llevar a cabo dentro de los controles de la red: el análisis del contenido del mensaje precisa tecnología que comprenda la aplicación p.ej. el sistema de correo electrónico. Sin embargo, las pruebas de contenido pueden impedir la apertura de numerosas brechas en seguridad, incluyendo la introducción de virus en la red corporativa (CAP GEMINI, Factbook Tecnologías de la Información, o.c., p. 358).

[44] RENZINI, R. *Les autoroutes de l'information: l'évolution technologique associée des moyens de sécurisation*. Vol. Le droit des autoroutes de l'information et du multimédia: un nouveau défi. Bruylant. Bruselas, 1997, pp. 212 y 213. A estos añadimos los sis-

Los servidores Web actualmente incluyen servicios de encriptación y autentificación del cliente, de modo que los usuarios puedan enviar y recibir datos con seguridad. Un servidor seguro le permite ser selectivo sobre quien puede recibir la información, para asegurarse de que la información sensible se conserva en secreto [45].

5. Conclusiones

La normativa sobre protección de datos personales se enfrenta en Internet a tres retos fundamentales: la vulnerabilidad, el carácter abierto de la red y la facilidad para realizar tratamientos invisibles (no conocidos por la persona concernida) sobre datos relacionados con la selección de contenidos o su identificación electrónica.

Si la red es vulnerable tanto a los ataques de terceros como a los errores o accidentes que puedan ocurrir en la transmisión de la información, ello se traduce, desde la perspectiva de la protección de datos personales, en la necesidad de adoptar especiales medidas de seguridad, como la utilización de procedimientos técnicos de cifrado y control de acceso a los archivos o informaciones que contengan datos de carácter personal o, incluso, la especial responsabilidad de los agentes involucrados en los tratamientos de datos realizados a través de la red.

El carácter abierto y global de Internet dificulta la sujeción de los tratamientos de datos personales a una normativa uniforme y generalmente aceptada por todos los países, obligando a acudir en la defensa de la vida privada de los usuarios a la cooperación internacional y a instrumentos adicionales de garantía de carácter autorregulatorio. Este carácter abierto y global de Internet favorece también la pérdida de control por el interesado sobre sus datos en Internet y propicia el reforzamiento de los derechos situados en la fase de recogida de los datos, de forma que el marco legal de protección de datos personales en Internet se articula incrementando las facultades de conocimiento y control del ciudadano en la salvaguardia de su derecho.

El control de los datos personales se perfila como la base de todo el sistema jurídico de protección de la persona frente a los riesgos inherentes a las nuevas tecnologías, por lo que también en Internet el sistema de protección de datos debe articularse con este contenido positivo de control, lo que se traduce en la necesidad de introducir procedimientos y sistemas mediante los cuales el titular de los datos que navegan o son accesibles por la red, pueda realizar efectivas actividades de control e invocar normas y utilizar procedimientos que involucren a los responsables de los tratamientos de datos personales en Internet.

La solución, en un plano internacional, pasa necesariamente por la cooperación de los países y la introducción de medidas nacionales complementarias. En el aspecto técnico son los propios intermediarios (operadores de red, proveedores de acceso, editores de software, servidores de páginas web o grupos de noticias) los que deben introducir sistemas técnicos (físicos y lógicos) que permitan al usuario el control y la decisión final sobre los tratamientos de los datos personales que les conciernan.

---

temas biométicos, de reconocimiento directo, sello y registros de comprobación (Para mas información *vid.* BARRIUSO, C. «La contratación electrónica». Dykinson, Madrid 1998, p. 247).

[45] HESLOP, B.; BUDNICK, L. Publicar con Html en inernet. Ed. Paraninfo. Madrid 1996, p.16.

Por último, un principio fundamental que debe regir el tratamiento de datos transaccionales en Internet, dentro de los cuales quedan incluidos los archivos de *logs, cookies* y los *clickstraim data,* es el del anonimato. Este principio puede ser exigido por el usuario basándose en los principios de finalidad y deber de cancelación contenidos en la legislación general sobre protección de datos y también en el deber de cancelación de los datos de tráfico y facturación, contenida en la legislación sectorial sobre protección de datos en el sector de las telecomunicaciones. El anonimato está ligado por un lado a la libertad de expresión y también a las facultades de control de los datos personales por su titular. Luego si es posible la comunicación anónima debe ser ofrecida al usuario para que pueda escoger entre comunicación anónima o en claro. También debe poder escoger el empleo de mecanismos que otorguen seguridad a sus comunicaciones en Internet.