CÓDIGO INVISIBLE Y PEQUEÑO GRAN HERMANO

Nuevas condiciones de posibilidad del derecho de protección de datos (*)

por

A. Daniel Oliver Lalana

Universidad de Zaragoza (**)

Resumen. Cuando apenas ha sido reconocido como un derecho fundamental autónomo, al derecho a la protección de datos se le exige inmediatamente adaptarse a nuevos retos surgidos en el entorno de Internet, tales como el tratamiento invisible y automático de datos del internauta o el auge de los proveedores de servicios que acumulan ingentes masas de información personal ("pequeños grandes hermanos"). Este trabajo discute cómo puede configurarse en este contexto hostil una suerte de derecho virtual a la protección de datos. En la reorientación del derecho de protección de datos hacia Internet, tres elementos parecen confluir en variadas combinaciones, de las que resultan a su vez diferentes niveles de protección. Estos tres elementos son: la tecnología misma (el llamado "código"), los mecanismos sociales de autorregulación y las normas jurídicas. Los tres constituyen las condiciones de posibilidad del derecho fundamental a la protección de datos en nuestra "sociedad web". En primer lugar, las conocidas limitaciones conceptuales y territoriales de los sistemas de regulación estatal parecen haber otorgado a los mecanismos de autorregulación un papel protagonista. Frente a las carencias regulativas del derecho estatal, la incorporación, en la propia tecnología y arquitectura de Internet, de los componentes esenciales del derecho de protección de datos se postula como un factor indispensable del derecho virtual a la protección de datos. En último término, y por primera vez en la historia, la protección de un derecho fundamental se anuda expresamente a la visibilización de un sistema tecnológico experto (Internet). Esto constituye un elemento esencial de una concepción normativa de la Sociedad de la Información concebida como una sociedad democrática tecnificada que informa reflexivamente sobre sus propios riesgos.

(*) Este trabajo es una reelaboración ampliada de la ponencia presentada al II Congreso Mundial sobre Derecho Informático (Madrid, 23-27 de septiembre de 2002).

(**) Profesor Asociado de Filosofía del Derecho; responsable del Módulo de Protección de Datos en el Master en Informática Jurídica de la Universidad de Zaragoza. http://www.unizar.es/derecho/fyd/oliverpd

0. INTRODUCCIÓN

En tiempos dominados por la ideología de la transparencia comunicacional (Lyotard 1979, 18), la protección de datos personales puede presentarse como una incómoda *excepción* frente a las *reglas generales* de la eficiencia administrativa y policial, del poder de control del empresario, o incluso de la libre iniciativa comercial. Mientras la Sociedad de la Información juguetea con un mal entendido ideal de transparencia, la protección de datos muestra en ciertos casos un halo de situación extraordinaria. Ejemplo de ello lo brinda la creciente tendencia a considerar la protección de datos como una barrera que dificulta la lucha eficiente contra el terrorismo (Working Party 53, 4) (1). Como el ingeniero D-503, protagonista de la novela de Zamiatin *Nosotros*, parece que también tengamos hoy que correr a la oficina de control, entregar al vigilante un billete de colores y recibir a cambio un certificado que nos permita bajar las cortinas (2). Aunque sean las cortinas virtuales.

Por fortuna, el panorama comienza a cambiar en muchos países (3) o, al menos, eso es lo que parece. Uno de los factores que han contribuido al cambio ha sido la consolidación del derecho a la protección de datos como un *derecho fundamental*. En el sistema jurídico español, como en otros países europeos, este derecho es resultado de una paulatina construcción constitucional, legislativa y, sobre todo, jurisprudencial (4), que ha encontrado el oportuno refrendo en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (Cumbre de Niza, 2000) (5). Hoy, liberado ya de su congénita servidumbre respecto de la protección de la intimidad (6), el derecho a la protección de datos se configura por fin como un derecho fundamental autónomo. Más aún: constituye *el* derecho fundamental característico de esa faceta del mundo social que comúnmente llamamos Sociedad de la Información, en la que opera como «un elemento constitutivo de la libertad del ciudadano» (7).

Todos sabemos bien que el reconocimiento jurídico y la declaración política son una cosa, y otra muy distinta es cómo darles acomodo en la realidad social. Y a este derecho

(1) Recordemos que ahora las compañías aéreas que operan en Estados Unidos han de transmitir los datos de cualquier pasajero a las autoridades de aquel país (cf. Working Party 66).

(2) «La linda O-90 debía llegar dentro de una hora (...). Corrí a la oficina de control, entregué al vigilante mi billete de color de rosa y recibí el certificado que me permitía bajar las cortinas. Ese derecho existe entre nosotros sólo para los días sexuales. De ordinario vivimos entre paredes transparentes, que parecen tejidas de aire rutilante, vivimos ante los ojos de todos (...). Eso facilita la dificultosa y eminente tarea de los Guardianes. (...) Es posible que esas extrañas viviendas opacas de los antiguos fueran la causa de su lamentable psicología. "Mi (sic!) casa es mi castillo" ¿Cómo llegaron a pensar tal cosa?» (Y. Zamiatin, *Nosotros*, anotación 4ª).

(3) Y no sólo en países europeos. Véase los arts. 15 de la Constitución de Colombia, 135 de la Constitución de Paraguay y 43 de la Constitución de la República Argentina. En este sentido, el reciente Dictamen del Grupo de Trabajo sobre el nivel de protección de datos en Argentina (Working Party 63) reconoce, con alguna salvedad, que este país ofrece un nivel adecuado de protección de datos.

(4) «Nuestro Tribunal Constitucional reconoce y protege ahora un derecho fundamental, el derecho de libertad informática (*sic*), que no figura en la Tabla del texto de 1978» (STC 292/2000, de 30 de noviembre, Voto Particular).

(5) Artículo 8. Protección de datos de carácter personal: «Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados 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 la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente». En principio, esta Carta no tendrá valor jurídico vinculante hasta la Conferencia intergubernamental del año 2004.

(6) Ahora recogido aparte en el artículo 7 (respeto a la vida privada y familiar) de la Carta de Derechos Fundamentales de la Unión Europea: «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones».

(7) *Declaración final de la Conferencia Internacional de Autoridades de Protección de Datos* (Declaración de Venecia): http://www.datenschutz-berlin.de/doc/int/konf/22/declar.htm. Véase también: Working Party 26, 3.

recién nacido le falta, precisamente, consolidación real. Esta carencia puede analizarse a propósito de la protección de datos en Internet. Apenas reconocido como derecho fundamental, al derecho de protección de datos se le exige su extensión y aplicación instantáneas a un mundo novedoso e hipercomplejo. Por ser "usuario" de la red, uno no deja de ser titular del derecho fundamental a la protección de datos, aunque los rasgos peculiares del entorno virtual parezcan imposibilitar su plena salvaguarda. Por ello, si es verdad que Internet es un «fértil caldo de cultivo para la transformación del Derecho» (Muñoz Machado 2001, 9), tal vez sea preciso reconstruir la protección de datos en línea como el primer *derecho fundamental virtual.*

En este proceso de reorientación, tanto los mecanismos de autorregulación, como la propia tecnología de Internet (lo que Lessig, como veremos, denomina "el código"), desempeñan un papel preponderante. Ambos constituyen las nuevas condiciones de posibilidad del derecho a la protección de datos personales cuyo análisis promete el subtítulo de este trabajo.

1. INTERNET Y LA INFORMACIÓN PERSONAL

1.1. Relación estática y dinámica de Internet con la información personal

Aunque gracias a Internet podemos realizar las acciones más diversas (8), la mayoría de nosotros la empleamos para buscar y obtener información, intercambiar mensajes electrónicos, o comprar y vender bienes y servicios (comercio electrónico). Los flujos de información implicados por estas actividades pueden contemplarse desde una doble perspectiva estática y dinámica. En el primer caso, Internet conforma un inmenso entramado de servidores que almacenan información ya creada y la ponen a nuestro alcance. Figurarse Internet como una fuente de datos de *acceso* irrestricto es la forma usual de considerar la relación del usuario con la información publicada en la red. Sería el caso de quien navega para obtener, por ejemplo, la fotografía del edificio en donde vive (9). Para obtener esta información es preciso que el usuario *se conecte* al servidor que la almacena. Esta segunda relación es ahora *dinámica*, en el sentido de que cada conexión genera necesariamente una información nueva, que antes no existía.

En Internet, tanto la información almacenada como la generada *ex novo* involucra datos personales y lo hace, además, en mayor grado que otros sistemas de telecomunicación. Como sabemos, el volumen de datos que son procesados por los sistemas de comunicación depende de la configuración o estructura de éstos. Por eso, además de atender al *tipo de actividades* desarrolladas en el entorno de Internet, también los especiales rasgos de su *arquitectura y configuración técnicas* han de tomarse en cuenta para comprender los nuevos problemas de la protección de datos.

(8) Como emular las aplicaciones *Messenger* o *ICQ* en la vida real, gracias al producto de localización *Find-A-Friend*, que las empresas Yahoo y CellPoint han diseñado para los teléfonos móviles. Véase: http://gartner3.gartnerweb.com/public/static/hotc/hc00088645.html

(9) http://fotos.qdq.com. Hasta hace poco, las llamadas guías inversas y multi-criterio acertaban siempre a vadear la disciplina jurídica.

1.2. Un ejemplo: el número IP

Tomemos el caso de la dirección del Protocolo de Internet (IP), quizá el "dato personal virtual" por antonomasia. Para que la información se transfiera correctamente del ordenador del usuario al servidor, es necesario un *protocolo* capaz de transportarla entre los distintos aparatos situados entre el usuario y dicho servidor. Como es sabido, la arquitectura de Internet descansa sobre una pareja de protocolos básicos, conocidos como TCP/IP (*Transmission Control Protocol/Internet Protocol*). Centrémonos en el protocolo de Internet, que es, por así decir, el "encargado" de los aspectos de identificación: a todo dispositivo conectado a la red se le asigna un número IP único que figura en todas sus comunicaciones, bien sea el origen (ordenador del usuario) o el destino de las mismas (servidor) (10).

A la luz del amplio concepto de dato personal que vertebra la legislación española (11), y en la medida en que el número IP puede vincularse a la identidad de una persona (cf. Corripio 2001; Working Party 37, 23), podemos considerar que este número es también un dato personal, como lo es cualquier número *identificador*, ya sea de máquinas (como el número de teléfono) o de individuos (documentos o cédulas de identidad) (12). Admitido esto, comienzan a surgir problemas. Cualquiera que sea la actividad que desarrolle el internauta, su ordenador estará siempre identificado por su número IP, que es un dato personal y como tal está sujeto a la legislación sobre protección de datos. Y ello, aunque ni el internauta ni muchos agentes de Internet lo sepan. Es cierto que, en principio, sólo el proveedor de acceso a Internet puede decirnos directamente a qué número de teléfono o a qué persona corresponde dicho número IP (13). Y no lo hará sin una orden del juez. Pero siempre existen caminos torticeros para vincular el número IP a la identidad de la persona, que dejan abierto el portillo de entrada al conocimiento de todo lo que hacemos en la red.

Desde luego, cabría aducir que no hay para tanto, que el número IP no es sino un dato de tráfico casi irrelevante porque, al referirse a una máquina, no revela información personal.

(10) Para simplificar, pensemos en una conexión ADSL, cuyo número IP es siempre el mismo, a diferencia de la conexión tradicional por módem (que opera con una dirección IP dinámica o variable). Normalmente, la arquitectura de un protocolo se representa en capas (Lessig 2001, 190 ss.). En la parte inferior, la capa de hardware corresponde a los cables y a las tarjetas utilizadas (*Ethernet*, por ejemplo); después, la capa de red administra la circulación de los paquetes a través de la red (IP); la capa transporte administra el flujo de datos entre dos máquinas (TCP); por último, la capa superior o *capa de aplicación*, administra los detalles de comunicación de una aplicación particular entre el servidor y el cliente (a esta capa pertenecen los protocolos *http*, para la navegación, *ftp* para la transferencia de archivos, o *nntp* para los grupos de noticias). En esta última capa se ventila, como veremos más adelante, un proceso de diálogo o "charloteo" entre el navegador (cliente) y el sitio web al que nos conectamos (servidor). Véase: http://www.cnil.fr/es/traces/demonst/es_demo.htm

(11) Véase el art. 3 de la Ley Orgánica 15/1999, de 15 de diciembre, de protección de datos de carácter personal (LOPD), y el art. 2.a de la Directiva 95/46/CE.

(12) En el sistema español, la identificación afecta a «cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada» (Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal).

(13) Los proveedores de acceso ocupan una posición privilegiada respecto del «tratamiento de los datos de conexión relacionados con una determinada dirección IP y pueden asociar dicha dirección IP con el conjunto de datos personales relativos al internauta, que es su cliente, por ello están sujetos a unas reglas especiales de destrucción de los datos de tráfico, de forma que sólo se les autoriza a conservar dichos datos con fines de facturación o para la promoción comercial de sus propios servicios con el consentimiento del usuario» (Corripio 2001). Sin embargo, la situación de algunos proveedores de servicios varía un tanto, habida cuenta de que ciertos de los servicios que ofrecen son gratuitos y por ello no parece tener sentido aplicar, sin más, el régimen de conservación de los datos previsto para la facturación telefónica. Véase el art. 65 del Real Decreto 1736/1998, por el que se desarrolla el título III de la Ley 11/1998 general de telecomunicaciones (en adelante, RGT).

Concedido, pero con dos salvedades. En primer lugar, los datos de tráfico, como otros datos aparentemente "inocuos", no dejan de ser datos personales. La amplitud del concepto básico de "dato personal" se debe justamente a que, con las técnicas de proceso y cotejo de información, no existe ningún dato irrelevante, por "inocuo" que sea su contenido informativo intrínseco. Como decía la Exposición de Motivos de la primera ley española de protección de datos de 1992, el conocimiento ordenado de *cualquier grupo de datos* puede dibujar un perfil de la persona; que puede ser luego valorado para las más diversas actividades, como la obtención de empleo, la concesión de un préstamo o la admisión en ciertos colectivos. Esta ley escribía así uno de los grandes monstruos de la protección de datos: las decisiones individuales automatizadas (cf. arts. 13 LOPD y 15 Directiva 95/46/CE), sobre las que volveremos luego.

En segundo lugar, los adelantos técnicos hacen que la distinción entre datos de tráfico y datos de contenido tienda a difuminarse. Así, una vez efectuada la "resolución" o conversión de este número en un nombre de dominio, podemos obtener información sobre el contenido de la comunicación o la visita realizadas, bien directamente, bien visitando la página correspondiente(cf. considerando 15 de la Directiva 2002/58/CE) (14). Es decir, si alguien conoce los números IP a los que me he conectado hoy (lo cual, en principio, "sólo" está al alcance de los proveedores de acceso y de servicios, incluyendo portales y buscadores) puede conocer también qué tipo de páginas que se esconden tras ellos, y por tanto conocer la naturaleza o el contenido de las comunicaciones. Como es obvio, todas estas posibilidades trascienden el concepto estricto de tráfico.

Si el protocolo más sencillo ya plantea éstos y otros problemas (15), en el caso de los llamados protocolos de alto nivel (por ejemplo, el *http*), cuyo funcionamiento precisa de un mayor intercambio de datos (cf. Lessig 2001, 190-92), la información generada es mayor y, por tanto, más sencilla resulta su vinculación con la persona (Working Party 37, 16) (16). En la gestión de peticiones *http*, por ejemplo, existe una variable que indica el nombre de la página desde la que se llega a la nueva página solicitada, de modo que los sitios web a los que nos conectamos podrían también rastrear el contenido de nuestras visitas anteriores a otras páginas.

Con sólo conectarnos a la red, la maquinaria del tratamiento de datos queda activada. Una vez dentro, la ecuación es casi de Perogrullo: cuanto más tiempo estemos en línea y cuanto más extensas sean las actividades que realizamos, mayor es el volumen de información personal del que dejamos rastro. Las imágenes del nuevo "panóptico" (Lyon 1994) y el "síndrome del pez" parecen bien cercanas.

(14) En cada una de las solicitudes *http*, es decir, cada vez que tecleamos una dirección (URL) en la barra de direcciones de nuestro navegador, el navegador lanza una solicitud al servidor de nombres de dominio (DNS), recupera de ahí la dirección IP del servidor al que solicita una página y contacta luego con dicho servidor.

(15) La "telepantalla" orwelliana o las "paredes de cristal" de Zamiatin no están tan lejos de la última versión del protocolo IP (IPv6), que permitirá 340 trillones de direcciones (en la versión actual, el IPv4, la cantidad de números IP es limitada) y vendrá incorporado en el hardware, de modo que cualquier dispositivo conectado a la red tendrá una identificación única, permanente y exclusiva.

(16) Explicación detallada y con ejemplos de la información generada en las conexiones TCP/IP y *http* en: http://www.cnil.fr/es/traces/demonst/es_parcour.htm. http://www.iec.csic.es/criptonomicon

2. ¿QUÉ PROBLEMAS *DE PROTECCIÓN DE DATOS* PLANTEA INTERNET?

2.1. Problemas de protección de datos

Como señala el Considerando 5 de la reciente Directiva 2002/58/CE, hoy se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales que crean necesidades específicas «en materia de protección de datos personales y de la intimidad de los usuarios». Pues bien, en el plano analítico, es conveniente diferenciar tres ámbitos de problemas asociados directa o indirectamente a la protección de datos personales del usuario de Internet.

El primero de ellos es el campo de la *recopilación y el tratamiento* de datos personales: un trasunto, en el entorno virtual, de la protección de datos tradicional. En segundo término, aparecen los problemas de la integridad, la confidencialidad y el secreto de las *comunicaciones electrónicas* (lo que incluye sistemas tan denostados como *Echelon*, *Carnivore* y *Enfopol*). Estas cuestiones se ubican a horcajadas entre el derecho de protección de datos y la protección de ciertos bienes iusfundamentales relacionados, en especial la intimidad y secreto de las comunicaciones (cf. Considerandos 2 y 11 de la Directiva 2002/58/CE). Por último, encontramos el ámbito de la *seguridad de los sistemas de información* y de los datos, el cual se proyecta sobre los dos anteriores. La seguridad de los sistemas de información es una preocupación relativamente independiente, aunque ahora está funcionalmente conectada con la protección de datos y la protección de la intimidad.

2.2. Protección de datos en sentido restringido

A continuación me centraré en los problemas que se presentan en el primer ámbito, que podemos llamar de *protección de datos en sentido restringido*. Pues bien, Internet presenta aquí cuatro facetas diferenciables (17). La conexión de un usuario a la red constituye un *servicio de telecomunicaciones*. Esta conexión discurre a través de los sistemas que gestionan los operadores de telefonía convencional o móvil, si bien puede utilizar el cable e incluso la red eléctrica (18). En la medida en que Internet es un servicio de telecomunicación, su uso genera datos personales sobre tráfico que, en principio, reciben una protección semejante a la otorgada por la ley a los datos de tráfico y facturación telefónica (19).

Ahora bien, a diferencia de estos últimos, que exclusivamente se refieren a la conexión en sí, los datos de tráfico en Internet pueden referirse indirectamente al contenido mismo de las comunicaciones (20). Así ocurre, por ejemplo, con el campo *subject* de las cabeceras de

(17) En sentido parejo, puede decirse que «la normativa sobre protección de datos personales en el sector privado 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» (Corripio 2001).

(18) http://www.endesanetfactory.com/castellano/proyectos_3.html

(19) Arts. 62 ss. del Real Decreto 1736/1998, por el que se desarrolla el título III de la Ley 11/1998 general de telecomunicaciones (en adelante, RGT).

(20) Con el servicio de identificación de llamadas (CLI) ocurría algo semejante, en cuanto que los datos de ciertas conexiones telefónicas revelan el contenido de las mismas, como es el caso de los llamados teléfonos eróticos. Por eso se prohíbe que éstos empleen este servicio de identificación (art. 76 RGT).

los mensajes electrónicos, o con determinados datos de navegación (Working Party 37, 55). En el preámbulo de la propuesta de reforma de la Directiva 97/66/CE se afirmaba que «es necesario separar la regulación de la transmisión de la regulación de los contenidos» (Considerando 7º) (21). Sin embargo, es evidente que esta separación *jurídica* no ha de resultar sencilla en la vida práctica.

Internet sirve asimismo como un canal o medio de recopilación de datos personales, y a su través pueden realizarse *operaciones visibles de tratamiento* de los mismos. Cada vez que rellenamos un formulario para abrir una cuenta de correo electrónico, que sucumbimos al denominado marketing de incentivos (promociones, sorteos...), o que nos registramos para emplear cualquier servicio, realizamos el mismo tipo de acto positivo de revelación de los datos que al completar un formulario en papel. A este respecto, Internet se asemeja a un "formulario mundial" de datos: cualquiera puede utilizar Internet para pedir a los usuarios sus datos personales, sin que importen ya ni el idioma ni las fronteras. Eso sí, con el añadido de que los datos se trasmiten a través de la red desde nuestro ordenador, directamente, a una base de datos.

En tercer lugar, la red "funciona" como una *fuente de datos de libre acceso* (22), y perfectamente se pueden recabar datos en ella sin que medie la intervención directa del interesado. Aunque se podría discutir mucho acerca de su carácter de "fuente de acceso público" (en tanto que medio de comunicación, *ex* arts. 3 LOPD y 2 Directiva 95/46/CE), lo cierto es que Internet pone *fácticamente* al alcance general los datos personales más diversos. De tal suerte, podemos obtener datos personales en guías y directorios, páginas personales, foros, cabeceras de mensajes electrónicos, publicaciones y prensa digitales, páginas institucionales...

Existe, por último, un amplio conjunto de *operaciones invisibles* de tratamiento, por lo general no consentidas, que supuestamente vienen implicadas por la configuración técnica de Internet. Hoy es casi imposible utilizar Internet sin verse confrontado con una serie de prácticas «que llevan a cabo todo tipo de operaciones de tratamiento de datos personales de manera invisible para el interesado» (Working Party 17, 3). En Internet, el mismo proceso de recopilación funciona siempre de ordenador a ordenador, lo que facilita el procesamiento de los datos. La diferencia radica ahora en que el internauta ni siquiera tiene que completar el formulario electrónico que visualiza en su monitor. Por eso en este caso el método es aún más lesivo, ya que pueden intercambiarse datos personales directamente entre ordenadores, y además sin que medie intervención, información o consentimiento del titular de los datos (23).

(21) El fragmento ha desaparecido de los Considerandos de la Directiva 2002/58/CE 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), que ha reemplazado a la Directiva 97/66/CE.

(22) El principio de finalidad, al impedir que incluso los *datos publicados* puedan utilizarse libremente para cualquier fin, cuadra mal con expresiones parecidas, como la de "datos públicamente disponibles". Conviene por ello sustituir el adjetivo "disponible" por otro más apropiado e inequívoco, como "accesible" (cf. Working Party 20, 3).

(23) Más sangrante aún es el caso del *spyware*, el software de control y software E.T. (Cohen 1999), que a veces se oculta tras los llamados programas de "acompañamiento" para navegación (Working Party 37, 53).

2.3. Ciudadano, consumidor, trabajador...

Por supuesto, esta clasificación no pretende ser exhaustiva. La protección de datos en Internet presenta numerosos problemas adicionales, como el control de los ordenadores una vez finalizado el acceso a Internet (*off-line*) (24). Sí me interesa resaltar que los problemas planteados surgen tanto en el ámbito público como en el privado. En el primero, cuando pensábamos que el derecho de protección de datos nos ofrecía cobijo suficiente frente al espíritu totalitario y el anhelo de omnisciencia del Estado, los adelantos en materia de gobierno electrónico han resucitado fantasmas que creíamos superados, e incluso han generado otros nuevos problemas de protección de datos impensables hace unos años.

Pero en el ámbito privado o empresarial las cosas no pintan mejor. Ya Lyon (1994, 169 ss. y 193 ss.) observaba cómo, ante al derecho a la privacidad, la categoría unitaria de "ciudadano" se ha atomizado en múltiples roles, como los de paciente, trabajador, consumidor, estudiante..., y que esto dificulta una eficaz salvaguarda del derecho. Pensemos en cómo los datos del consumidor, y más aún los del consumidor electrónico, son vorazmente tratados y empleados por las empresas. Otro tanto parece ocurrir en el ámbito de las relaciones informativas entre trabajador y empresario: como apunta Castells (2001) «la protección de la privacidad no se extiende al mundo del trabajo, bajo el control de la organización corporativa».

3. *INTERNET LAW* Y PROTECCIÓN DE DATOS

Todas estas cuestiones atinentes a la protección de datos han de enmarcarse, a su vez, dentro un problema general que afecta a todas las actividades de la red. Me refiero a la regulación o derecho de Internet (*Internet Law*). El campo de la protección de datos ofrece una buena muestra de esta dificultad añadida de reglamentar jurídicamente las actividades realizadas en el nuevo entorno. Rasgo peculiar del derecho fundamental a la protección de datos es, como veremos, que su salvaguarda no puede limitarse simplemente a las normas jurídicas (estatales). Este rasgo merece ser subrayado: ¿imaginan que algún otro derecho fundamental no estuviera suficientemente amparado por la legislación estatal?

En lo esencial, este problema proviene de los caracteres constitutivos de Internet, de la pluralidad de ámbitos normativos implicados y de la dificultad que supone transponer los conceptos jurídicos tradicionales a las actividades de la red. Estos caracteres son responsables, en último extremo, de un significativo desplazamiento hacia las normas privadas.

3.1. Características estructurales de Internet: extraterritorialidad

Es ya lugar común decir que los rasgos constitutivos de Internet la convierten en un mundo que a duras penas admite disciplina jurídica (Muñoz Machado 2000, 37 ss. y 153-54; Lessig 2001, 57 ss.). El ciberespacio avanza siempre más deprisa que las instituciones jurídicas, y su *carácter proteico* y constante mutabilidad hacen de él una "realidad" difícil de

(24) Esto afecta sobre todo a los equipos compartidos y, por ejemplo, respecto a los llamados archivos *cache*, al software que facilita completar formularios, al acceso *off-line* a las *cookies*...

regular. Quizá la mayor –y más tempranamente advertida– dificultad del derecho de Internet es la *extraterritorialidad*. El verbo "ir" posee en el ciberespacio un sentido distinto a que tiene en el espacio real (Lessig 2001, 53). Esta circunstancia hace que, en ocasiones, el usuario crea estar facilitando sus datos personales a una entidad cuando en realidad es otra, no identificada y radicada en otro territorio, la que los está obteniendo (25).

Las categorías de espacio y tiempo son muy endebles en el la red, y esto alimenta en la mente del usuario, sentado solo frente al monitor, una *sensación de libertad y anonimato*. El *websurfing* causa la sensación de moverse sin frenos, sin restricciones de ningún género y, sobre todo, «sin que se atisbe en ninguno de los rincones que se visitan el menor rastro de los poderes públicos o privados» (Muñoz Machado 2000, 35). Ensimismado, el internauta olvida que también acata algunas reglas *sui generis*, un código o regulación *técnica* de Internet. Como dice Lessig (2001, 207), no es la naturaleza quien determina el ciberespacio, sino el código: «el hardware y el software, que hacen del ciberespacio lo que es, regulan el ciberespacio tal como es» (Lessig 2001, 25). Y aunque lo parezca a veces, la técnica nunca es neutral, sino que puede tener serias implicaciones normativas, éticas y políticas (26).

3.2. Necesidad de coordinación normativa

Excluir una herramienta de transferencia de información personal tan importante como Internet del ámbito de aplicación de las normas jurídicas sobre protección de datos carecería de justificación (cf. Comisión Europea 2002, 9). Por eso, ante este panorama, contamos con un nutrido marco normativo de referencia, compuesto por normas de derecho internacional (27), de derecho comunitario europeo o de derecho nacional, y de normas privadas o de autorregulación. En punta de lanza, tenemos las normas generales de protección de datos (Directiva 95/46/CE, LOPD) y las normas sobre protección de datos en el sector de las telecomunicaciones (Directiva 97/66/CE, RGT).

Con todo, estas normas carecen hasta la fecha de la necesaria especificidad y tecnicidad para adaptarse a Internet, y de ahí que trate de legislarse *ad hoc*. Al hacerlo, hay que asumir que el tipo de regulación posible de la red, si existe alguno, tiene que ser variado y proyectarse sobre múltiples contenidos (Muñoz Machado 200, 35). Esto es particularmente cierto en sede de protección de datos. Consecuencia del enfoque omnicomprensivo y transversal que tiene este derecho es que se extiende por todos los sectores del ordenamiento. Un mismo sitio de comercio electrónico puede tener que afrontar problemas de derecho de consumo, de telecomunicaciones, de firma electrónica, de protección de datos; estar vinculado por contratos de *housing* o *hosting*, logística y atención telefónica (*outsourcing*)...

(25) Recomendación de la APD al sector del comercio electrónico para su adaptación a la LO 15/1999, disponible en: https://www.agenciaprotecciondatos.org/recomendaciones.htm

(26) Por ejemplo, son "técnicas" las normas que limitan el tamaño (4 Kb) y el número de *cookies* (300) que el navegador puede almacenar en el disco duro del usuario: http://www.ietf.org/rfc/rfc2109.txt, http://www.cookiecentral.com/faq, http://www.netscape.com/newsref/std/cookie_spec.html

(27) Destacan, entre estas últimas, los Convenios del Consejo de Europa, como reciente sobre cibercrimen: cf.: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm

De ahí que, por usar la expresión de la Directiva de comercio electrónico (2000/31/CE), sea preciso un tratamiento normativo "coordinado" que tenga en cuenta que también otras disposiciones pueden afectar a la protección de datos personales en diversos aspectos. Y así, por ejemplo, en cuanto a la protección de los consumidores (Directiva 97/7/CE), a la publicidad comercial electrónica (2000/31/CE; Ley española de Servicios de la Sociedad de la Información) o al uso de seudónimos en la firma electrónica (Real Decreto-Ley de Firma Electrónica).

3.3. Dificultad de trasladar los conceptos jurídicos al mundo virtual

La tercera gran barrera de regulación atañe a la *aplicabilidad de determinados conceptos-clave* de la legislación sobre protección de datos al entorno de Internet. Se ha discutido si conceptos esenciales como el de *dato personal* del art. 3 LOPD o el de *identificabilidad* del art. 3 R.D. 1332/1994 son aplicables al número IP e incluso al e-mail; si la distinción entre *datos de tráfico y de contenido* es válida también para las comunicaciones de Internet (28); o si Internet es o no es una *fuente de acceso público* en el sentido técnico-jurídico. A este último respecto, y pese a la reticencia general (y a la interpretación de la Agencia Española de Protección de Datos), entiendo que la respuesta es afirmativa: Internet es una fuente de acceso público en tanto que medio de comunicación (*ex* art. 3 LOPD). Lo cual no quiere decir, como ha repetido *ad nauseam* el Working Party, que los datos de acceso público sean de libre e irrestricta utilización por cualquiera (Working Party 33). Para ellos valen, sobre todo, la regla del equilibro de intereses y el principio de finalidad (29).

Y otro tanto puede decirse de los sujetos intervinientes en el procesamiento de datos personales. Junto –o "frente"– al usuario individual, hemos de contar siempre con la diversidad de agentes o participantes en Internet. Éstos pueden desempeñar tres roles básicos: el de operador de telecomunicaciones, el de proveedor de acceso y el de proveedor de servicios. Los "servicios", dentro de este último concepto, son de toda condición. A los muy conocidos motores de búsqueda, portales de acceso, sitios de comercio electrónico o empresas de estadísticas de navegación, pueden sumarse, por ejemplo, los "informediarios" (Hagel/Singer 1999; Working Party 37, 91 ss.) y los proveedores de agentes inteligentes de software.

De esta multiplicidad de posibles responsables de los ficheros deriva el problema de la segmentación de roles a los efectos del tratamiento de los datos. Muchos de ellos desempeñan conjuntamente, en la práctica, funciones que jurídicamente están divididas. Algunos proveedores de servicios de Internet operan, a un mismo tiempo, en calidad de proveedores de acceso, proveedores de contenidos, buscadores, portales, servicios de correo web u otros servicios de valor añadido, como la elaboración de estadísticas de navegación o visitas. Ha-

(28) Se duda, a este respecto, si las *cookies* constituyen un "medio" de tratamiento de datos que no sea simplemente un medio de tránsito en el sentido del art. 5.1. LOPD. De ser así, el responsable de la *cookie* debería aplicar nuestra legislación y designar en España un representante. Todos estamos de acuerdo en que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas y «que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados» (Considerando 20 de la Directiva 95/46/CE). Pero ¿quién hará que una empresa de cibermarketing ubicada en Singapur aplique la Ley española de protección de datos?

(29) Véase: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pd_en.htm

bida cuenta de la dificultad práctica de deslindar el tráfico del contenido, la aplicación de las distinciones legales presenta dificultades sobreabundantes (cf. Working Party 37, 29).

3.4. Privatización regulativa

La consecuencia más destacable que viene anudada a esta situación es la progresiva cesión de parcelas de regulación al sector privado. El carácter abierto y global de Internet dificulta «la sujeción de los tratamientos de datos personales a una normativa uniforme», y por ello «obliga 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» (Corripio 2001). En una palabra, la adaptación de la legislación a Internet parece presuponer la cesión de parcelas normativas a los agentes que operan en el entorno virtual.

Lo malo es que en la desigual lucha entre la tecnología y la autorregulación, de una parte, y la legislación, de otra, vienen a imponerse las primeras. Quizá, podemos añadir, por ese fenómeno de irradiación alentado por el predominio estadounidense en el mundo virtual. Las normas privadas, influenciadas por los sistemas anglosajones de impropiamente llamados "de autorregulación", son más sencillas y eficaces, aunque ofrecen menos garantías que las normas comunitarias y nacionales.

Al cabo, Internet termina por afectar a principios esenciales como los de información y consentimiento, de finalidad y de derecho al olvido (conservación); al ejercicio de los derechos del ciudadano; y a la articulación de los procedimientos oficiales (tutela, tribunales), que vienen paulatinamente a ser reemplazados por "garantías privadas" de cumplimiento de la ley, cuyo ejemplo más aquilatado es el principio séptimo del Acuerdo de Safe Harbor (30).

4. HERMANOS PEQUEÑOS, CÓDIGO Y *ONLINE PROFILING*

4.1. Acumulación y utilidades de la información personal

Desde hace algún tiempo, oímos hablar del auge de los "pequeños grandes hermanos", un siempre creciente número de compañías que acumulan cada vez más datos de sus clientes actuales o potenciales. A día de hoy, las compañías doblan su volumen de datos almacenados cada dieciocho meses (31). La coalición de la tecnología con los mecanismos de identificación y vigilancia configura un sistema en el que quien tenga la posibilidad *legal* o *fáctica* de acceder a los datos «puede conocer lo esencial de los que cada persona hace en la red y fuera de ella» (Castells 2001).

Al crecer los datos generados e intercambiados merced a Internet, crece también el interés por transmutarlos en significado útil, información o conocimiento. Siendo Internet un mercado gigantesco, las empresas que operan en ella no van a permitir que millones de clien-

(30) http://www.export.gov/safeharbor/sh_overview.html

(31) En materia de bases de datos existe un "Club del Terabyte", un grupo de 120 empresas vinculadas a IBM, cuyos *data warehouses* almacenan cada uno más de un exabyte de datos. Fuentes de IBM señalan con orgullo que este club tiene veinte miembros más que su más cercano "competidor del terabyte": http://www.as400.ibm.com/developer/bi/newsclip.html.

tes potenciales naveguen por ahí sin saber lo que éstos hacen o dejan de hacer. La información acumulada en Internet facilita la elaboración de un perfil completo de la persona, y ello sin que el internauta pueda siquiera sospecharlo. Bajo el punto de vista de las empresas, el objetivo fundamental de la elaboración de perfiles en línea es, sencillamente, la supervivencia: «quien posea los derechos sobre los perfiles de los clientes será quien determine los ganadores y los perdedores de esta nueva era» (Hagel/Singer 1999, xiii).

Con ese designio general, los pequeños grandes hermanos pueden confeccionar y usar los perfiles, al menos, para tres finalidades.

La primera y, a lo que parece, más comprensible, es el *(i) diseño de la estrategia comercial*, es decir, la realización de predicciones de consumo y ventas, así como la promoción y el marketing personalizado. Pero a esta finalidad tan legítima se asocian dos utilidades adicionales que suscitan más de un reparo ético y jurídico. Me refiero, de una parte, a la *(ii) adopción de decisiones individuales automatizadas* en ámbitos tan diversos como el mercado laboral y financiero (aplicación de técnicas de *scoring*), el terreno de la prevención y represión de delitos, o el control de publicación de contenidos nocivos (cf. Working Party 50 63, 62). Y, de otra, a una tercera finalidad, que viene ya de camino, y que con el barbarismo de turno podríamos llamar *(iii) net classing*, esto es, la restricción del uso de los servicios de Internet basada en la adopción de decisiones individuales automatizadas que implican la previa estratificación o segmentación socio-económica de los usuarios de Internet (32).

En efecto, habida cuenta de que la industria del cibermarketing financia muchos sitios web (*e.g.* buscadores), no es disparatado pensar, a partir de ahora, que algunas empresas recurrirán a la elaboración y uso de perfiles personalizados para garantizar que servicios hasta entonces supuestamente "gratuitos" queden fuera del alcance de «quienes no dispongan de un nivel suficiente de ingresos o no hayan respondido a cientos de *pancartas* publicitarias» (Working Party 37, 21). En el mismo saco entrarían quienes, simplemente, desean proteger su privacidad y adoptan al efecto medidas que impiden la recopilación indiscriminada de sus datos. El "ciberuniverso igualitario" podría resultar así desplazado por la estratificación o segregación de base económica (33). Según apunta Wolton (2000, 106), las desigualdades socioculturales que Internet estaba llamada a mitigar, pueden reaparecer de nuevo, y con mayor crudeza, en el futuro inmediato del ciberespacio.

Como he dicho, una vez registrada la masa de información, es preciso darle algún significado comercialmente utilizable. A tal fin se cuenta con herramientas de minería de datos o *data mining* (34), que automatizan el proceso de obtención de información relevante entre las masas de datos de todo tipo que generan los flujos de comunicación en Internet. Así puede obtenerse información útil donde no parece haberla. Cualquiera que acceda lícita o

(32) Un ejemplo de este tipo de decisiones es el llamado *web-lining*: sitios web que restringen sus servicios a usuarios con un perfil de escasas compras o compañías que ofrecen sus productos a precios más caros a determinados grupos (Federal Trade Commission 2000, 13).

(33) Lessig (2001, 285-86) ejemplifica este problema a propósito de los programas de fidelización de las compañías aéreas que operan en la red.

(34) http://www.dmg.org. El nombre evoca la imagen de quien encuentra metales preciosos en una montaña aparentemente sin valor alguno.

ilícitamente a una cantidad relevante de datos anónimos podría "minarlos" y conectarlos con personas identificables (Federal Trade Comission 2000, 12). El resultado será un perfil detallado que sirve para predecir los gustos, necesidades, preferencias y hábitos del internauta. Un ejemplo típico del servicio que presta la minería de datos es el marketing orientado a objetivos (*targeted marketing*) y la fidelización de los clientes, que permite a la compañía oferente personalizar los anuncios (35).

4.2. Mercantilización de los datos personales

Sin duda, los datos personales son un negocio para las empresas que los poseen y por eso tratan de incorporarlos a sus activos. Pero esto puede suscitar cuestiones graves desde el punto de vista de la legislación vigente en Europa. Pensemos si no en el problema que el controvertido régimen de la cesión de datos acarrea en un ámbito de competencia tan feroz, donde las fusiones, quiebras y absorciones son el pan diario (cf. Gauthronet 2001; Miravet/Baches 2001). Al fundirse las empresas se confunden sus bases de datos y crece la preocupación por el acopio desmesurado de los mismos (Working Party 37, 75) (36). Al final, la información personal se ha convertido en la moneda del ciberespacio (Markoff 1999). ¿Cómo se explica si no que la conocida compañía de cybermarketing DoubleClick atesore más de cien millones de perfiles de cliente? ¿O que su homóloga Engage cuente con 800 campos o categorías de interés entre sus más de 50 millones de perfiles? (Federal Tade Comisión 2000, 6). Es verdad que los datos personales siempre han sido, de alguna forma, un medio de pago, pero es que en el mundo del ciberespacio son la moneda común. El esplendor de los "pequeños grandes hermanos" depende, precisamente, de que lo sigan siendo.

4.3. Del "código" al perfil

Para saber de dónde proviene la información que nutre las bases de minería de datos no basta con referirnos al tratamiento visible de los datos (muchas veces alentado por el marketing de incentivos), ni tampoco a la relación estática con la información personal (utilización de Internet como fuente de libre acceso). Es necesario volver sobre la arquitectura y la configuración de Internet. En efecto, y aun cuando no siempre exista un trasfondo malevolente o ilícito, lo cierto es que resulta bien sencillo pasar de la arquitectura de Internet al *on-line profiling*. Es un hecho innegable que la configuración técnica de las cosas determina sus posibilidades de utilización y condiciona también, por tanto, a sus usuarios, sean o no cons-

(35) En este contexto han de verse asimismo las aplicaciones CRM para gestión de las relaciones con el cliente (CRM: *Customer Relationship Management*), cuya finalidad es conocer más del cliente para "fidelizarlo" (cf. Curry/Curry 2002). Frente al problema del "cliente infiel y promiscuo", "hay que recoger, analizar y sacar resultados de la información extraída a los clientes para poder sacarle el máximo rendimiento", dado que para que este tipo de aplicaciones sea eficaz resulta vital que «toda la organización participe en la obtención y análisis de todas las experiencias que un cliente tiene con la marca o empresa». Véase http://www.fecemd.org/archivos/crm.pdf

(36) «Little Brother is more banal. In the new surveillance world, it's no longer the FBI agent hunkered down in a listening van tracking your every word but rather the local Safeway manager or Federal Express Corp. database administrator who has access to the details of your life as a consumer. But unlike the FBI agent, these watchers don't care who you are: it's what you buy and what you eat that interests them» (Markoff 1999).

cientes de ello. La arquitectura de Internet y la elaboración de perfiles en línea comparten, por así decir, invisibilidad e inadvertencia.

Como sabemos, la naturaleza de la red viene determinada por sus arquitecturas (Lessig 2001, 67). Éstas son expresadas en una suerte de "código", término ya célebre con el que Lessig (2001, 192-93) designa las aplicaciones de hardware y software que funcionan sobre los protocolos TCP/IP. A poco que ampliemos la acepción que Lessig confiere al término, éste comprendería todo el conjunto de elementos integrantes de la configuración técnica de las comunicaciones en el ciberespacio. De este modo, pertenecerían al código, además de los protocolos TCP/IP y los protocolos de alto nivel (*http, ftp*...), todos los programas y aplicaciones que los emplean (navegadores, clientes de correo...). De donde podemos decir que, por ejemplo, el charloteo del navegador (*chattering*), los hipervínculos invisibles y las *cookies* son *elementos del código* de los que sacan partido las compañías publicitarias en Internet. Como también lo es ya, y con consecuencias aún imprevisibles, la polémica versión 6 del número IP (IPv6) a la que aludía antes.

A esto hemos de sumar, del lado del internauta, que la *configuración por defecto* de los productos de la red suele ser siempre la que menos garantías ofrece desde el punto de vista de la protección de datos (37). Y la cuestión no es magra: si ya el usuario, por lo común, no es consciente de que sus datos personales se han recopilado, y tampoco de que pueden usarse con intenciones que le son desconocidas (Working Party 17, 4), entonces la configuración por defecto de los productos cobra una incidencia decisiva sobre el nivel general de protección de datos en línea (Working Party 11, 3) (38). Y aquí las prácticas de los proveedores de servicios pueden llegar a ser escandalosas.

En ocasiones, el peligro de la venta directa es mayor que la mera incomodidad que provoca al navegar. Las compañías de cibermarketing no sólo ofrecen publicidad, sino que reúnen y sistematizan, mediante *cookies* y *web bugs* (39), los datos de quienes visualizan sus pancartas. En cierto modo, esta información es anónima. Pero puede vincularse con la identidad de la persona y agregarse a información identificable, por ejemplo, en el momento en que ésta complete un formulario en la página de una compañía publicitaria, o en otro sitio web que ceda los datos a la misma. Las políticas de privacidad de algunos proveedores de servicios comienzan advertir del riesgo de esta personalización de los datos (40). Pero, aun con todo, cualquier compañía que opere en la red puede aún recopilar información de modo invisible y elaborar con ella un perfil del internauta.

(37) En el acuerdo de licencia de una aplicación de charla (*chat*), podemos leer: «Please note that *in each and every Internet application, the IP address of the sender is an integral part of the TCP/IP standard protocol* of the Internet, and *can be extracted by any party to the communication session* using certain software and/or hardware. Also note that the IP privacy feature, designed to allow an ICQ user to reduce the exposure of his/her IP address on ICQ, is provided to you *as a convenience only* and does not guarantee a complete non-exposure of your IP address». (La cursiva es mía).

(38) «El servicio de correo web gratuito de Microsoft (Hotmail), que cuenta con más de 110 millones de internautas registrados en todo el mundo (3 millones en España), ofrece la información personal de sus usuarios a empresas. (...) Si no se desactivan dos nuevas casillas de su perfil, (...) Microsoft cede sus datos de forma automática». http://www.elmundo.es/navegante/2002/06/17/empresas/1024305127.html. Véase también: http://www.libertaddigital.com/noticias/noticia_73571.html

(39) http://www.bugnosis.org

(40) Especialmente interesante resulta a este respecto la política de privacidad de Nedstat, disponible en: http://www.nedstat.com/es/f80276e120501p121091_index.htm

Entre unas cosas y otras, se ha recabado –y continúa recabándose– en Internet gran cantidad de datos personales sobre los usuarios, sin su conocimiento ni por tanto su consentimiento. Esto se debe sobre todo a la actuación invisible de la tecnología. Valga un ejemplo: más de la mitad de los usuarios de Internet han abierto ya alguna vez *banners* situados en los servidores de sólo tres compañías: DoubleClick, Engage y 24/7 Media (Federal Trade Comisión 2000, 3). Por lo que hace a la protección de datos, el código ha incrementado las asimetrías entre ciudadanos y responsables de ficheros. Con Lessig (2001, 263), podemos preguntarnos: ¿podrá el mismo código volver a restaurar el equilibrio?

5. AUTORREGULACIÓN, NORMAS JURÍDICAS Y TECNOLOGÍAS DE PROTECCIÓN DE DATOS

La solución a los problemas de protección de datos (en sentido restringido) que suscita Internet, en especial por cuanto hace a su configuración técnica ("código"), puede seguir tres caminos: el de la tecnología, el del derecho y el de la autorregulación.

5.1. Tecnología

Frente a las amenazas que para la protección de datos se desprenden de la configuración técnica de Internet, la primera respuesta la ofreció Internet misma. Desde su nacimiento, «a las tecnologías de control y vigilancia se contraponen tecnologías de libertad» (Castells 2001). En sede de protección de datos, esta solución técnica lleva el nombre de las tecnologías favorecedoras de la privacidad o PET's (*Privacy Enhancing Technologies*). Estas tecnologías han sido definidas como un sistema de medidas técnicas que protegen la privacidad eliminando o reduciendo los datos personales que se facilitan en Internet, o impidiendo el tratamiento innecesario o no deseado de los mismos; todo ello sin que se pierda la funcionalidad del sistema informático en el que operan esos datos (Borking/Raab 2001) (41). A título individual, el Internauta siempre ha dispuesto de herramientas tecnológicas para protegerse. Los llamados "anonimizadores" de navegación, la criptografía y los repetidores de correo pueden contarse como las primeras reacciones libertarias de los internautas.

Los productores informáticos extrajeron pronto su propia lección de estas reacciones. Las empresas que comercializan herramientas y programas para Internet saben que cada vez más usuarios toman conciencia del problema y están dispuestos a pagar a cambio de protección. Y es que, como observa Corripio (2001), son ellas quienes «deberán proporcionar las herramientas necesarias para que el usuario pueda ejercitar un control de los tratamientos de datos que le conciernen».

El objetivo último que guía a las empresas que diseñan especificaciones meramente técnicas de protección de datos es hallar la forma en que las máquinas negocien nuestras

(41) La categoría es muy amplia y heterogénea: abarca desde los anuladores de *cookies* y los detectores de *web-bugs*, hasta los repetidores de correo y los anonimizadores de navegación, pasando por los servidores *proxy*, los agentes de software y las aplicaciones criptográficas (PGP)

preocupaciones en materia de protección de datos. Se busca, en una palabra, la forma de delegar el proceso de negociación en un agente inteligente de software o en un protocolo destinado a "negociar" las protecciones de privacidad (Lessig 2001, 294-95). La industria de Internet ha querido sumarse activamente a esta tendencia, y lo ha hecho con un proyecto de arquitectura favorecedora de la privacidad: la Plataforma de Preferencias de Privacidad (P3P) (42). Esta plataforma permite a los sitios web expresar sus prácticas de privacidad en un formato estándar de modo que puedan ser leídas e interpretadas automáticamente por un agente de software que utiliza el usuario. Éste no precisa leer las políticas de privacidad de los sitios que visita, pues lo hace el software en su lugar, al tiempo que comprueba si tales prácticas coinciden con las preferencias de protección de datos previamente definidas por el usuario (43). Hoy, y por lo menos en un sentido amplio, puede decirse que también las PETs forman parte del código de Internet.

La integración técnica de ciertos principios de protección de datos se ha revelado insuficiente en muchos casos, y el de la Plataforma de Preferencias de Privacidad es uno de ellos. Una plataforma técnica para la protección de datos no basta por sí sola para proteger el derecho a la protección de datos en la red. En primer lugar, uno puede sospechar que, al funcionar automáticamente, este tipo de herramientas podría camuflar u ocultar información relevante desde el punto de vista de la protección del ciudadano.

Los flujos de datos y su relevancia iusfundamental podrían así mantenerse ocultos, al socaire de un sistema cuya finalidad es que el usuario "no tenga que preocuparse" por leer las políticas de privacidad de los sitios que visita. Pero sobre todo, «es necesario aplicarla en un contexto de normas jurídicas «que sean ejecutables y deparen a todas las personas un nivel mínimo y no negociable de protección» (Working Party 11, 2). Hace falta, en suma, «una solución que vaya más allá del código» (Lessig 2001, 290). En efecto, si debe introducirse en la arquitectura de la red un nuevo estándar de protección de datos, no será el mercado quien lo incluya. El poder del mercado no estará detrás del cambio (Lessig 2001, 301).

5.2. Normas jurídicas (estatales)

El segundo camino de solución lo marca la legislación oficial. Al tratar del *Internet Law*, he mencionado las dificultades generales que suscita esta posibilidad (§ 3). Con el consabido problema de la territorialidad, la legislación europea sobre protección de datos debe aplicarse a los datos recabados con equipos, informatizados o no, situados en el territorio de la Unión Europea o del Espacio Económico Europeo (art. 4.1 Directiva 95/46/CE). Y esto cubre desde luego el tratamiento invisible. Pero también el temido perfil en línea queda al alcance de la norma.

(42) Funciona como una lista de preguntas y respuestas sobre el nivel de privacidad entre nuestro navegador y el sitio web al que nos conectamos. http://www.w3.org/P3P, http://www.research.att.com/projects/p3p/. Recientemente, han aparecido en el mercado las dos aplicaciones de privacidad, *Tivoli Privacy Wizard* (http://www.tivoli.com/products/solutions/security/news.html) y *PrivacyBird* (http://www.att.com, http://www.privacybird.com). Este software sólo funciona para las páginas web que utilizan P3P.

(43) Sólo el navegador Internet Explorer 6 permite el empleo de P3P, lo cual es irrespotuoso con el ideal de neutralidad tecnológica asumido por las legislaciones europeas. Con todo, esta Plataforma comienza a ser utilizada por los sitios web más populares (cf. Adkinson/Eisenach/Lenard 2002, 26).

Las normas de protección de datos son suficientemente flexibles para ese fin. Según recuerda el Grupo de Berlín (44), los derechos del ciudadano se extienden también a los perfiles, hayan sido éstos elaborados en línea o por medios tradicionales (45).

Lo cierto es que el enfoque omnicomprensivo de la legislación sobre protección de datos permite (o exige) su ampliación prudencial a ámbitos nuevos como el del tratamiento invisible de datos personales. Los principios de lealtad y transparencia, tan importantes en la recogida *visible* de los datos, quizá bastaran para hacer que el tratamiento *invisible* salga de algún modo a la luz. Con todo, hasta ahora, veíamos cómo las normas de protección de datos perdían vigor al contacto con el código. Pero nadie se rasgaba las vestiduras jurídicas por el código en sí. Ahora ya nos hemos dado cuenta de el código de Internet está en gran medida involucrado en la protección de datos personales. La gestión de las solicitudes *http*, los hipervínculos invisibles o las *cookies* dan muestra de ello. Por eso, una de las formas de regular la protección de datos en Internet sería regular directamente el código (Lessig 2001, 90).

El código es de carácter privado (Lessig 2001, 401) y no se puede limitar sin más (cf. Working Party 17). Las normas europeas de protección de datos no pueden intervenir de esta forma tan directa, puesto que deben sujetarse al principio de neutralidad tecnológica que inspira hoy cualquier regulación jurídica de los problemas de la Sociedad de la Información. La directivas europeas sobre protección de datos son, por ello, tecnológicamente neutrales, ya que lo dispuesto en ellas no incide directamente sobre el tipo de tecnología utilizada y se aplica también «con independencia de los medios tecnológicos empleados en el tratamiento de datos personales» (Comisión Europea 2002, 9).

La tendencia actual, más bien, y toda vez que no es fácil la actuación normativa directa sobre el código, es ordenar su visibilización. Así lo hace la nueva Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. También el Grupo de Trabajo del Artículo 29 en materia de protección de datos (*Working Party*) ha querido identificar las medidas concretas que habrán de aplicar los agentes participantes a fin de garantizar que el tratamiento de los datos en línea es lícito y leal. Estas medidas «se centran especialmente en cuándo, cómo y qué información debe facilitarse al interesado, pero añaden detalles prácticos sobre otros derechos y obligaciones procedentes de las Directivas» (Working Party 43, 4). Aumentar la transparencia del código, en este contexto, no quiere decir otra cosa que ofrecer al usuario la posibilidad de que conozca y valore las operaciones invisibles que éste realiza (46).

(44) http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm

(45) El derecho de acceso comprende tanto los datos de base como «los resultantes de cualquier elaboración o proceso informático« (Instrucción 1/1998, de la Agencia Española de Protección de Datos, Norma 2.7). Véase arts. 13 y 15 y ss. LOPD. Los principios aplicables a la elaboración de perfiles en línea «son aquellos que tradicionalmente corresponden al ámbito de la protección de datos personales» (Corripio 2001).

(46) Como observa Lessig (2001, 407), «lo máximo que podemos esperar de la regulación del código en el ciberespacio «es un equilibrio negociado entre transparencia y efectividad».

5.3. Autorregulación

En esta desesperada búsqueda de soluciones, se afianza una tercera vía: los mecanismos de autorregulación. Juegan éstos un papel principalísimo. Ahora bien, ¿estará preparado nuestro derecho de protección de datos para asumir que su eficaz regulación *jurídica* depende de la *autorregulación social*? Para despejar esta incógnita hemos de diferenciar entre dos formas de "autorregular" la protección de datos en Internet. En sentido impropio, puede decirse que la autorregulación es la simple autoorganización normativa de los agentes de Internet. Que sean los propios participantes quienes se "auto-regulen" no supone novedad alguna (cf. Lessig 2001, 293). Allá donde no llega la norma jurídica, la sociedad se provee desde siempre de herramientas de regulación propias.

Esa es la visión "anglosajona" del término. Conforme a ella, cualquier política de privacidad de una empresa podría ser entendida como un mecanismo de autorregulación. Ocurre, por desgracia, que las políticas de privacidad de la mayoría de las compañías estadounidenses que operan en la red son poco más que una declaración (*statement*) de intenciones, por demás no muy ambiciosa. Tan sólo en supuestos excepcionales, este tipo de políticas son controladas por las autoridades gubernamentales, y en todo caso este control se verifica a través de las normas que regulan el correcto funcionamiento del mercado y no como un problema de derechos fundamentales de la persona (47). En este sentido, barrunto que a muchos les gustaría ver la protección de datos como un elemento sujeto a la propiedad del interesado, negociable por tanto en los mismos términos que cualquier otro bien (cf. Lessig 2001, 296-99). Pero esto implica desatender su naturaleza de bien jurídico fundamental y, por tanto, (relativamente) indisponible. Puede pensarse que, si se generaliza esta opción –paremos mientes en el Acuerdo de Safe Harbor–, la protección dista mucho de ser óptima (48).

En sentido estricto, la autorregulación, como un fenómeno característico del Estado del Bienestar, denota en puridad el "control jurídico" de la autorregulación social. Esto es, el diseño de un marco de derecho cogente dentro del cual los agentes sociales involucrados puedan dotarse de las normas específicas que quieran. De lo que se trata ahora, en definitiva, es de regular jurídicamente los mecanismos de autorregulación social (Teubner 1989, 91 ss.). Este es el sentido del artículo 32 LOPD, así como el de otros muchos ejemplos de "derecho reflexivo" vigentes en nuestro ordenamiento.

También el mercado ha ofrecido muestras de que de este tipo de mecanismo regulativo es posible sin detrimento del nivel de protección de datos garantizado por la legislación europea. Por ejemplo, en ausencia de disposiciones legislativas específicas, el Código de @ECE supuso un adelanto en cuanto a la identificación y tratamiento jurídico del problema planteado por el uso de *cookies* (49). La elaboración de mejores prácticas (*best practices*) de conducta administrativa y empresarial empieza a ocupar la posición clave de esta vertiente de autorregulación (Working Party 37, 94-95). Incluso existen ya instituciones destinadas a

(47) La Comisión Federal de Comercio (FTC), junto con el Departamento de transportes (DT), cada uno en su ámbito de competencia, vendrían a ser algo así como un equivalente muy desnaturalizado de las autoridades europeas de protección de datos.

(48) Un indicador del nivel de garantías que ofrece el Acuerdo de Safe Harbor es la temprana adhesión al mismo de DoubleClick, Inc.: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

(49) http://www.aece.org/docs/codigoetico.doc

orientar a los empresarios y administraciones públicas en la elaboración de programas, sellos y políticas de privacidad que especifican para algún sector concreto de actividades el marco normativo oficial, respetándolo por ende meticulosamente (50).

La vertiente garantista de la *autorregulación* todavía va más lejos en Internet. No sólo permite adoptar normas (privadas) de protección de datos, sino que sólo a su través es posible incidir indirectamente sobre el código. Ahí reside su mayor utilidad (51). No basta con establecer marcos normativos para los agentes privados, sino que hay que incorporar los principios de protección de datos al software usado en la red. Para ello tratan de diseñarse nuevas tecnologías en favor de la privacidad que se ocupen de evitar las invasiones en la privacidad, gestionando la protección de datos con el límite del mínimo no negociable que garantiza nuestro régimen tuitivo. Es decir, el desafío estriba en cómo transponer la legislación de protección de datos, en su vertiente europea (que es el estándar de protección de datos más alto del mundo) a las especificaciones de los productos, para que luego éstas sean incorporadas mediante programación informática (52). En definitiva, *son los 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 conciernen* (Corripio 2001).

Si esta incorporación del nivel europeo de protección a la misma tecnología no puede condicionarse directamente mediante normas jurídicas, quizá, al menos, pueda venir por la vía de la autorregulación.

6. EL DERECHO FUNDAMENTAL VIRTUAL A LA PROTECCIÓN DE DATOS

6.1. Implicaciones del carácter fundamental del derecho a la protección de datos

En sus decisiones y sentencias, la Comisión Europea y el Tribunal Europeo de Derechos Humanos han elaborado y definido un derecho fundamental basándose en distintos derechos humanos vinculados a la protección de datos de carácter personal. Puede decirse que en la cúspide del modelo europeo de protección de datos (53), al que se acomoda el sistema español, está el reconocimiento de este derecho como un derecho fundamental asociado a la dignidad de la persona. Ocupa este reconocimiento una posición clave. Algunos países europeos han integrado este derecho fundamental en su constitución, mientras que, en otros, la protección de datos ha adquirido estatuto de derecho fundamental a través de la jurisprudencia (54). La mencionada Carta de Derechos Fundamentales de la Unión Europea ha culminado este proceso.

(50) Véase: http://www.surveillancecommissioners.gov.uk/index.html

(51) Llegados hasta aquí, las normas jurídicas se difuminan en recomendaciones y consejos sobre la utilización de técnicas favorecedoras de la privacidad. Quizá sea el reconocimiento de su propia inhabilidad para afrontar la plena dimensión de estos problemas.

(52) La última tendencia apunta hacia los agentes inteligentes de protección de privacidad (Borking 2000).

(53) http://www.datenschutz-berlin.de/doc/eu/konf/01_fund_rights.htm

(54) Con mayor circunstanciamiento que la STC 254/1993, de 20 de julio, la STC 292/2000, de 30 de noviembre (FJ 7°) explica cómo «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un

Frente a la hostilidad del medio, el reconocimiento del derecho de protección de datos como un derecho fundamental tiene una consecuencia inmediata. Su ligazón con la dignidad de la persona y su pertenencia privilegiada al orden constitucional otorgan al derecho de protección de datos (relativa) prevalencia sobre otros derechos e intereses amparables. Ya en el mismo plano conceptual, la protección de datos *no puede ser* un obstáculo para la consecución de fines valiosos. Y desde luego no puede ser presentada como tal.

Por lo pronto, porque la salvaguarda efectiva de cualquier derecho fundamental redunda en beneficio de la totalidad del orden colectivo. Una de las virtualidades de los derechos fundamentales es que constituyen elementos de igualación y legitimidad social (55). Parafraseando la Sentencia del Tribunal Constitucional Federal Alemán sobre la Ley del Censo (BVerfGE 65, 1), puede decirse que la protección de datos integra el bien público, en la medida en que constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos. La misma idea refleja el Considerando 2 de la Directiva 95/46/CE al declarar –en un tono casi esencialista– que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos.

Desde luego, el de protección de datos no es un derecho absoluto. Esto no es un demérito, porque los derechos absolutos no existen. Pero su carácter fundamental, como digo, le confiere una prioridad relativa o *prima facie* sobre otros bienes constitucional o jurídicamente amparados. En especial, y aunque puede colidir con otros derechos fundamentales e intereses públicos, es el aspecto comercial el que plantea mayores problemas cotidianos. La protección de datos reviste gran importancia económica y muchos la consideran un obstáculo al comercio o una barrera no tarifaria (*non-tariff barrier*) (56). Sin embargo, las restricciones al derecho de protección de datos deben ser siempre administradas con extrema cautela (*in dubio pro derecho humano*). Máxime cuando el grado de desconocimiento general favorece la lesión inadvertida del derecho (57).

6.2. Necesidad de un derecho fundamental "virtual"

Probablemente, el derecho a la protección de datos es el derecho fundamental que mayor relevancia reviste en el ciberespacio. No es, desde luego, el único. Pero la relación de

particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos».

(55) En este sentido, entre otras muchas funciones, el derecho a la protección de datos coadyuva a evitar la discriminación y la estratificación socioeconómica de los usuarios de Internet.

(56) Véase el art. XIV lit. c ii del Acuerdo General Sobre Tarifas y Servicios de la Organización Mundial del Comercio (WTO-GATS): http://www.wto.org/english/tratop_e/serv_e/2-obdis_e.htm.html

(57) Esto es especialmente relevante a los efectos del equilibrio de intereses señalado por los artículos 6.4 LOPD y 7 de la Directiva 95/46/CE.

Internet con otros derechos fundamentales es más bien instrumental. La libertad sindical o el derecho de sufragio (en el caso de que llegue a funcionar el *e-voting*) podrán vulnerarse *mediante la intervención sobre* el vehículo o instrumento de la comunicación. Pero en el caso de la protección de datos, es el mismo funcionamiento (código o arquitectura) de la red el que representan ya, por sí mismo, una amenaza. No hace falta que exista una actuación dirigida específicamente a vulnerar la protección de datos personales. En cierto sentido, ésta se vulnera sola. El normal funcionamiento de Internet afecta a principios fundamentales que forman parte, incluso, del contenido esencial del derecho de protección de datos según lo ha definido nuestra jurisprudencia constitucional. Valgan algunos ejemplos.

En primer lugar, la configuración técnica de la red no debería permitir el acopio indiscriminado e invisible de datos personales, sino sólo de aquellos que sean necesarios para la prestación de los servicios de telecomunicación (principios de necesidad, proporcionalidad y adecuación). Como recuerda el Considerando 30 de la Directiva 2002/58/CE, «los sistemas para el suministro de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que se limite la cantidad de datos personales al mínimo estrictamente necesario».

El segundo gran reto de la protección de datos en Internet es cómo articular la restricción de los usos secundarios (principio de finalidad). Este problema juega en tres ámbitos esenciales: *(i) en la gestión de las comunicaciones*, supone la prohibición de elaborar perfiles identificados sobre la base de los datos de tráfico; *(ii) en el tratamiento visible* de los datos, la mayoría de los proveedores de servicios hacen una interpretación exageradamente laxa del principio. Basta con mirar las políticas de privacidad en la red para darse cuenta; por último, *(iii)* este principio guarda especial importancia en el campo de los *datos públicos* (Working Party 20, 3). Los datos públicamente accesibles en la red se sujetan a los principios de necesidad, finalidad y equilibrio de intereses. En contra de lo que se piensa, la legislación sobre protección de datos también se aplica a los datos publicados (Working Party 20, 4; Working Party 37, 60).

El tercer principio nuclear que resulta lesionado es el principio de transparencia, que tenemos que ligar a la necesidad de visibilización del código y a la capacitación del ciudadano para autodeterminarse informativamente (principio del consentimiento). Los agentes participantes de Internet deben hacer visible el tratamiento automático de los datos que generan las comunicaciones de Internet. Si el carácter abierto y global de la red favorece la pérdida de control por el interesado sobre sus datos, ha de propiciarse, como propone Corripio (2001), 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 base en el incremento de las facultades de conocimiento y control del ciudadano en la salvaguardia de su derecho.

Con demasiada frecuencia, se olvida que también la protección de datos en Internet 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 pueda realizar efectivas actividades de control (Corripio 2001). La nueva Directiva de protección de datos en materia de telecomunicaciones sigue esta línea de ideas plenamente, como muestra el tratamiento del ya viejo problema de las cookies. Según declara en su Considerando 25, su uso para fines legítimos está justificado a condición de *que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar*

que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un «chivato» (cookie) o dispositivo semejante.

En otras palabras, los proveedores de acceso y de servicios deben publicar de forma comprensible todas las explicaciones que sean precisas para que los usuarios reconozcan la estructura de la red o el servicio, las posibles responsabilidades que puedan derivarse, la cantidad y naturaleza de los datos procesados y sus posibles cesiones (58).

El derecho de protección de datos en línea tiene, por último, que adaptar determinados conceptos al nuevo entorno. Como hemos mencionado, la multiplicidad de agentes que operan en la red debe tratar sólo aquellos datos personales que les correspondan en función de su rol, y nunca agregar todos los datos obtenidos (pensemos en los supuestos de externalización o *outsourcing*: logística, servicios fuera de línea...). Se trata, en suma, de procurar una suerte de equilibro o separación de poderes informativos. Algo similar ocurre con la distinción entre datos de tráfico y de contenido. Suele considerarse la recopilación y tratamiento de los primeros plantea menores problemas que la de los segundos: los datos sobre la hora, la duración y el volumen de la comunicación parecen revelar poca información acerca de la persona. Sin embargo, hay otros datos de tráfico que ya no son tan inocuos. Así, entre otros muchos, la fuente o el destino de la comunicación (las páginas web visitadas), o el campo *subject* de los mensajes electrónicos, merecen mayor protección. La recopilación y agregación de todos estos datos puede, en algunas situaciones, permitir la elaboración de un perfil de los intereses de la persona, de sus contactos sociales y de su contexto social (59).

7. ESPECIFICACIÓN TECNOLÓGICA DEL DERECHO A LA PROTECCIÓN DE DATOS

El funcionamiento de la red y el comportamiento de sus agentes, siempre en pugna por la supervivencia, representan un riesgo para el nivel de garantías del ciudadano y por tanto para el orden constitucional. Este riesgo debería compelernos de seguido a corregir las graves asimetrías informativas entre usuarios de Internet y proveedores de acceso y servicios. Las normas de protección de datos, así como su interpretación, han de orientarse a neutralizar estos riesgos específicos. En el plano jurídico, por lo tanto, «el sistema de protección de datos personales en Internet se debe articular mediante el reconocimiento de un haz de derechos específicos que recojan la particular fisonomía de los riesgos que, en este sector, padecen los usuarios» (Corripio 2001). Esto supone reorientar el derecho de protección de datos para obtener un "nuevo" derecho virtual a la protección de datos, que algunos denominan *virtual right to be let alone* (60). En realidad, como hemos visto al desglosar los elementos afectados, los materiales para construir este derecho específico estaban ya al alcance prudencial.

(58) http://www.datenschutz-berlin.de/doc/int/iwgdptc/tc_en.htm

(59) Cf. arts. 14-15 de la Convención del Consejo de Europa sobre Cibercrimen: http://conventions.coe.int

(60) http://www.datenschutz-berlin.de/doc/int/iwgdptc/tc_en.htm En este sentido, Corripio (2001) vertebra el nuevo derecho en torno a un principio de anonimato.

Lo que verdaderamente tiene de "nuevo" este derecho es la integración técnica del estándar europeo de protección de datos. La idea de trasfondo es bien sencilla: si que el modo en que el código cambia depende de los autores del código, «el modo en que los autores del código lo modifican puede depender de nosotros» (Lessig 2001, 207). El futuro de la protección de datos exige articular tecnologías para el aseguramiento de los objetivos normativos establecidos en el plano legislativo (cf. Kilian 2002, 152). Corresponde pues *instar* a los agentes que intervienen en la arquitectura de la red ofrecer al usuario productos que respeten la privacidad (Working Party 37, 22). Esta opción puede verse como una tecnificación del derecho fundamental o, rizando la expresión, como la "juridificación fundamental" del código. Ciertas tecnologías favorecedoras de la privacidad, en especial algunos agentes inteligentes de software, son un ejemplo de esta integración técnica (Borking 2000). Pero hay muchos otros.

Así, «resultaría útil que el principio de finalidad pudiese integrarse en determinados medios técnicos. Esto podría considerarse también una forma de tecnología a favor de la privacidad» (Working Party 37, 53). Y no se pide tanto. En el caso de bases de datos en-línea, pueden limitarse técnicamente sus posibilidades de utilización como se ha hecho en el caso de las guías y directorios telefónicos, donde los criterios de búsqueda deben «permitir únicamente la presentación de un número limitado de resultados por página» (Working Party 33, 6). También modificar las configuraciones por defecto de los productos de software sería un gran avance: en un entorno marcado por las deficiencias de cultura de protección de datos, distribuir productos que por defecto permiten tratamientos no informados ni consentidos de datos personales equivale a promover dichos tratamientos.

En palabras de Corripio (2001), el sistema específico de protección de datos en Internet incluye el derecho a realizar opciones informadas sobre el tratamiento de los datos personales, el derecho al anonimato y el derecho a ser informado de la falta de seguridad y a adoptar los instrumentos técnicos de seguridad. Desde luego, no será fácil configurar ni jurídica ni prácticamente estos derechos. Al menos, no mientras la cuestión de la regulabilidad de Internet siga sin respuesta. En un entorno sin fronteras, el usuario debería tener también el derecho a recurrir ante una autoridad transnacional con poderes de investigación y aplicación, algún mecanismo de resolución internacional de disputas (61).

En esta materia, las regulaciones de base territorial no tienen sentido alguno (Muñoz Machado 2000, 181). Un correcto marco regulativo de la protección de datos en Internet presupone usuarios activos y conscientes que sean capaces de ejercitar sus derechos en una sociedad de la información donde el tráfico de datos personales no conoce fronteras (Schartum 2001, 167).

Internet no puede ser un ámbito *fácticamente* excluido ni un campo de excepción a la legislación sobre protección de datos. El internauta sigue siendo titular del derecho fundamental de protección de datos a todos los efectos. Sólo en la medida en que los problemas de aplicación territorial del derecho a Internet afecten a la protección de datos es lícito excepcionar nuestras normas Pero fuera del espacio virtual "europeo" no acaban los recursos. La

(61) Un cuerpo supranacional podría ofrecer servicios coordinados de protección de datos en el entorno Internet (Schartum 2001, 168).

autorregulación y la integración técnica de los principios, y en especial la prudencia del internauta, pueden ofrecer garantías de protección de datos allá donde el principio de territorialidad no tiene cabida. Bien entendido que la autorregulación de la red debe ser, en materia de protección de datos, una autorregulación controlada (derecho reflexivo), no una simple organización privada de las cosas (62).

8. CONCLUSIÓN

La incorporación de las tecnologías de la información y las telecomunicaciones a la cotidianeidad de nuestras actividades ha destapado la endeblez de ciertos derechos fundamentales de nuevo cuño, como el derecho a la protección de datos. Al ser éste un derecho indisociablemente ligado al desarrollo tecnológico, sus contenidos concretos deben acompasarse al nivel de incorporación de este desarrollo a la vida cotidiana. De otra forma, el derecho proclamado en abstracto queda inerme frente a las amenazas anudadas al desarrollo tecnológico. Por ello, y sin olvidar que tal vez en un futuro próximo serán necesarias nuevas modificaciones, hoy la tarea prioritaria es transponer a Internet el derecho a la protección de datos.

En este proceso de reorientación, tres elementos confluyen en variadas combinaciones, de las que resultan a su vez diferentes niveles de protección. Estos elementos son la tecnología misma sobre la que opera Internet (el "código"), los mecanismos de autorregulación y las normas jurídicas. Al presentarlos como las nuevas condiciones de posibilidad del derecho fundamental a la protección de datos, he querido significar que la aspiración ético-normativa condensada en este derecho no puede alcanzar un grado de satisfacción adecuado si desatiende alguna de ellas. Ahora bien, lo que se postula no es cualquier suerte de combinación de los tres elementos, porque no son del mismo rango. De una parte, son las normas jurídicas las que deben determinar el área de operación de los mecanismos de autorregulación. De otra, tanto las normas estatales como las privadas deben proyectarse, condicionándola, sobre la tecnología estructural de Internet.

Si, como hemos visto, la protección de datos en Internet queda en buena medida asociada al código, el derecho de protección de datos dependerá entonces de la visibilización del "código" invisible. Habida cuenta de las dificultades para actuar directamente sobre éste, el primer paso necesario es hacerlo más visible, especificando así el principio tradicional de transparencia en materia de protección de datos. Sólo de esta forma podrá recuperar el internauta la parte de la autodeterminación informativa que pierde al conectarse a la red. Y sólo así pueden corregirse las asimetrías que median entre los pequeños hermanos y los ciudadanos. Este nuevo equilibrio pasa por la información y el conocimiento que tienen los segundos sobre las posibilidades de tratamiento de su información por parte de los primeros.

Pero más allá de esto, y quizá por primera vez, la protección de un derecho fundamental del individuo aparece ligada a la visibilización de un sistema experto: el sistema de las tele-

(62) Hasta la Comisión Federal de Comercio de los EE.UU. parece coincidir en esto al postular, en su Informe sobre privacidad correspondiente al año 2000, el control y la regulación de la autorregulación: http://www.ftc.gov/reports/privacy2000.pdf. Véase también el reciente trabajo de Kilian (2002, 159).

comunicaciones y, en concreto, de Internet. En este sentido, como decíamos antes, Internet puede servir para contribuir al cambio. Pero también puede no hacerlo. Con ello, invocamos uno de los principios esenciales para la salvaguarda de los derechos humanos de tercera generación: los ciudadanos deben involucrarse activamente en la protección de su propio derecho. Algunos escépticos vislumbran dificultades para lograrlo (Schartum 2001, 169). Y no les faltan buenos indicios para ello: la anhelada participación del ciudadano exige tal vez demasiada información. Pero es que la Sociedad de la Información debe ser, ante todo, una sociedad que reflexivamente informa sobre sus propios riesgos.

Referencias

- Adkinson, W., J. Eisenach y T. Lenard (2002), *Privacy Online: A Report on the Information Practices and Policies of Comercial Websites*, Washington, The Progress & Freedom Foundation, Disponible en: http://www.pff.org
- Borking, J. (2000) *Proposal for building a privacy guardian for the electronic age*, La Haya, Registrariekamer. Disponible en: http://www.registratiekamer.nl/bis/content-1-1-9-5-7.html
- Borking, J. and Raab C, «Laws, PETs and Other Technologies for Privacy Protection», 2001 (1), *The Journal of Information, Law and Technology* (JILT) http://elj.warwick.ac.uk/jilt/01-1/borking.html
- Castells, M. (2001), «Internet: ¿una arquitectura de libertad? Libre comunicación y control del poder», Conferencia inaugural del curso académico 2001-02 de la Universitat Oberta de Catalunya (UOC), http://www.uoc.es/web/esp/launiversidad/inaugural01/internet_arq.html
- Cohen, A. (2000), «Spies among us», en *Time (Europe)*, vol. 156, no. 5 (July 31, 2000), disponible en http://www.time.com/time/europe/digital/2000/09/future.html
- Comisión Europea (2002), *Protección de Datos en la Unión Europea*, Bruselas. Disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/news/guide.htm
- Corripio Gil-Delgado, R. (2001), *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*, Madrid, Premio Agencia de Protección de Datos (cederrón).
- Curry, J. y A. Curry (2002), *Customer Relationship Management. Cómo implementar y beneficiarse de la gestión de las relaciones con los clientes*, Barcelona, Gestión-2000.
- Federal Trade Commission (2000), *On-line profiling: A Report to Congress* (June 2000), disponible en http://www.ftc.gov/os/2000/07/onlineprofiling.pdf
- Gauthronet, S. «The Future of Personal Data in the Framework of Company Reorganisations», *23th International Conference of Data protection Commissioners*, Paris, 2001.
- Hagel, J. y M. Singer (1999), *Net Worth: Shaping Markets When Customers Make the Rules*, Cambridge-MA, Havard Bussines School Press.
- Kilian, W. (2002), «Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung?», en: *Freundesgabe für A. Büllesbach*, Stuttgart, J.F. Steinkopf Druck.

- Lessig, L. (2001), *El código y otras leyes del ciberespacio*, Madrid, Taurus.
- Lyon, D. (1994), *El ojo electrónico. El auge de la sociedad de la vigilancia*, Madrid, Alianza.
- Lyotard, J.F. (1979), *La condición postmoderna*, Madrid, Cátedra, 1994.
- Martín Pallín, J.A. (1998), «El número de identificación único», *Jueces para la Democracia*, núm. 33 (1998), pp. 7-17.
- Muñoz Machado, S. (2000), *La regulación de la red. Poder y Derecho en Internet*, Madrid, Taurus.
- Markoff, J. (1999), «The Privacy Debate: Little Brother and the buying and selling of consumer data», disponible en http://www.upside.com/texis/mvm/print-it?id=36d4613c0&t=1
- Miralles, S. y S. Baches, «La cesión de datos de carácter personal. Análisis de la legislación vigente y su aplicación a determinados supuestos prácticos», *LA LEY* núm. 5306 (11.05.2001), pp. 1-7.
- Pérez Luño, A.E. (1991), «Las generaciones de derechos humanos», *Revista del Centro de Estudios Constitucionales* 10 (1991), 203-217.
- Schartum, D.W. (2001), «Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects», *International Review of Law, Computers and Technology*, pp.157-170.
- Teubner, G. (1989), *Recht als autopoietisches System*, Frankfurt, Suhrkamp.
- Téllez Aguilera, A. (2001), *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Madrid, Edisofer.
- Wolton, D. (2000), *Internet ¿Y después? Una teoría crítica de los nuevos medios de comunicación*, Madrid, Gedisa.

Documentos del Working Party (Working Party)

Todos los documentos del Grupo de Trabajo sobre protección de datos del Artículo 29 (*Working Party*) pueden consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

- Working Party 66: *Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States (24.10.2002)*
- Working Party 65: *Working Document on Black Lists* (3.10.2002)
- Working Party 64: *Dictamen 5/2002, sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones* (11.10.2002)
- Working Party 63: *Opinion 4/2002 on the level of protection of personal data in Argentina (3.10.2002)*
- Working Party 53: *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism* (14.12.2001).

– Working Party 43: *Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea* (17.05.2001).

– Working Party 37: *Privacidad on-line. Enfoque comunitario integrado de la protección de datos en línea* (21.11.2000).

– Working Party 33: *Dictamen 5/2000, sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio* (13.07.2000).

– Working Party 26: *Dictamen 4/1999, sobre la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales* (7.09.1999).

– Working Party 20: *Dictamen 3/1999 sobre la información del sector público y la protección de datos personales* (3.05.1999).

– Working Party 17: *Recomendación 1/1999 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware* (23.02.1999)

– Working Party 11: *Dictamen 1/1998, sobre la Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS)* (16.06.1998).