El derecho al anonimato en Internet

POR **RAMÓN M. ORZA**

En el texto se propone la configuración del derecho al anonimato -consagrado legalmente en el ámbito de las comunicaciones telefónicas, pero muy discutido en el ámbito de Internet- como uno de los nuevos derechos fundamentales vinculados a la Red

Es generalmente admitido que los antecedentes literarios de una sociedad conectada por redes y ordenadores en la que la información es la materia prima, se sitúa en el año 1984, cuando se publicó la novela *Neuromancer* de William Gibson[1]. Este descarnado relato refiere, en una visión futurista y fantástica, el modo de vida en una sociedad totalmente invadida por los ordenadores y las redes que los unen. En ella aparece por primera vez el término *cyberspace* para describir un espacio virtual -no físico- determinado por la interconexión de personas a través de redes telemáticas.

Afortunadamente, la evolución de las redes informáticas no ha ido por esas vías, pero sí es cierto que Internet[2] como realidad fáctica está imponiendo de manera evidente una serie de modificaciones en el ámbito jurídico, al romper muchos moldes y obligar a una nueva lectura de muchas de las categorías y conceptos jurídicos.

En efecto, la eclosión de las Tecnologías de la Información y la Comunicación (TIC) y todas las derivaciones que existen a su alrededor (correo electrónico, mensajería instantánea, foros, videoconferencias, etc.) están obligando a reelaborar muchos derechos y libertades tradicionales, pero desde perspectivas y posibilidades absolutamente nuevas y desconectadas de las definiciones al uso, cuando se dotaron de contenido teórico muchos de los conceptos y definiciones que aparecen en nuestros textos constitucionales.

Derechos propios de la Sociedad del Conocimiento

Fundación Telefónica
Telefónica

Por tanto, aunque el debate sobre la necesidad de incorporar al orden jurídico nuevos derechos fundamentales no es nuevo en la teoría jurídica, sí es cierto que debería reforzarse en estos momentos. En la actualidad se plantea con enorme fuerza la necesidad de definir otro nuevo conjunto de derechos a incluir en los textos constitucionales, vinculados a lo que empieza a conocerse como la Sociedad del Conocimiento y que vayan más allá de la mera protección de los datos personales o de una adaptación más o menos forzada de los derechos tradicionales. Así, la extensión del secreto de las comunicaciones a las comunicaciones electrónicas, la garantía de un cierto derecho al anonimato cuando se navegue por Internet, se hagan transacciones económicas o se participe políticamente a través de la Red, aparece como uno de los más importantes, a la vez que más discutidos, en la actualidad.

De hecho, en este ámbito, además de las regulaciones oficiales, también es necesario tener en cuenta la aparición de reguladores privados diferenciados de los aparatos tradicionales del Estado (Administración pública, policía, tribunales), que poseen -y de modo creciente- un enorme poder. Por poner algunos ejemplos, la fuerza que pueden tener los proveedores de acceso o de contenido a la Red o la posibilidad que tienen buscadores como Yahoo, Google, Bing o Msn (Microsoft) de establecer mecanismos de censura privados o de conocimiento o divulgación de informaciones privadas, incluso de manera opaca, sin conocimiento por parte de los ciudadanos o de las Administraciones Públicas nacionales, pueden suponer una enorme amenaza para el ejercicio de las libertades ciudadanas. Tampoco hay que dejar de lado las amenazas que se presentan para los ciudadanos a través de los rastreos que se pueden realizar de su navegación o del contenido de su correo electrónico. Además, cada día aparecen nuevos problemas derivados del uso generalizado de las nuevas redes sociales, tipo MySpace, Facebook, Tuenti o Twitter, por citar solo algunas, que implican a miles de ciudadanos, entre ellos a muchos menores de edad.

Pero todo ello solo puede ser un incentivo para que desde el ámbito jurídico constitucional nos ocupemos continuamente de esta ‘nueva frontera’ de los derechos fundamentales, donde se están construyendo las bases de la sociedad futura y en la que hay que tener en cuenta nuevos retos, como pueden ser la superación de las fronteras físicas entre los Estados, la dificultad de perseguir los sitios de Internet situados extraterritorialmente, las diversas concepciones de la libertad de expresión o las dificultades procesales para la persecución de las infracciones y delitos cometidos a través de la Red.

Pero el camino para la incorporación a los textos constitucionales de estos nuevos derechos nunca es fácil ni rápido. De hecho, es común la resistencia de las constituciones a las reformas (la idea de la rigidez constitucional), por lo que se ha tenido que acudir con frecuencia a la vía jurisprudencial para dotar de protección a estas nuevas necesidades, puestas normalmente de manifiesto por la doctrina o por la práctica.

A ello se refería concretamente el magistrado del Tribunal Constitucional español Jiménez de Parga cuando en un voto particular a la Sentencia del Tribunal Constitucional español 290/2000, de 30 de noviembre, indicaba que «no ha de sorprendernos que en la Constitución española de 1978 no se tutelase expresamente la libertad informática [ya que] veintidós años atrás, la revolución de la técnica en este campo apenas comenzaba y apenas se percibía»[3]. Y ello supone un problema, pues «a diferencia de lo que ocurre en otros textos constitucionales

Fundación Telefónica
Telefónica

(por ejemplo, en los de Portugal o Argentina, siguiendo la senda de la Constitución de Estados Unidos de América) nuestra Ley Fundamental de 1978 no incluye una cláusula abierta, después de haber consignado una amplia lista de derechos y libertades».

Junto con la jurisprudencia, también sería posible que estos eventuales nuevos derechos tuvieran acogida en tratados y convenios internacionales, que dadas las características transnacionales de estas TIC, aparecen como un medio especialmente idóneo. De hecho, la regulación de los nombres de dominios, e incluso la creación de un cierto 'gobierno de Internet', exigen la colaboración internacional[4]. Un ejemplo constante de esta vía puede ser la labor legislativa -a través del Derecho originario (los Tratados) o del Derecho derivado (elaborado por sus propios órganos)- de la Unión Europea.

El derecho al anonimato[5]

Este es uno de los derechos que suelen ser cuestionados con mayor intensidad en los debates sobre nuevos derechos de la sociedad de la comunicación. Pero no nos cabe ninguna duda sobre el hecho de que su protección y mantenimiento deben constituir una garantía para el ejercicio de las libertades públicas, del mismo modo que lo son también el secreto de las comunicaciones o la protección de datos. Sin embargo, si observamos la evolución legislativa en esta materia no parece que debamos ser especialmente optimistas.

De hecho, aunque no sea directamente extrapolable, es significativo que la Directiva de la UE 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) fuera muy cuidadosa a la hora de garantizar el anonimato en llamadas telefónicas ante la posibilidad de que los operadores de telefonía pudieran comunicar el número desde el que se llama a la hora de establecer una conexión telefónica. Así, en su parágrafo 34, la Directiva señala: «Es necesario, por lo que respecta a la identificación de la línea de origen, proteger el derecho del interlocutor que efectúa la llamada a reservarse la identificación de la línea desde la que realiza dicha llamada y el derecho del interlocutor llamado a rechazar llamadas procedentes de líneas no identificadas», lo que se justifica por el hecho de que «Determinados abonados, en particular las líneas de ayuda y otras organizaciones similares, tienen interés en garantizar el anonimato de sus interlocutores»[6].

Y de hecho, el artículo 8 de esta Directiva establece que «1. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al usuario que efectúe la llamada la posibilidad de impedir en cada llamada, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen. El abonado que origine la llamada deberá tener esta posibilidad para cada línea. 2. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al abonado que reciba la llamada la posibilidad, mediante un procedimiento sencillo y gratuito, siempre que haga un uso razonable de esta función, de impedir la presentación de la identificación de la línea de origen en las llamadas entrantes», bien que con la posibilidad de eliminar esta opción en determinados casos (Directiva 2002/58/CE, art. 10)[7].
Esta Directiva fue trasladada al derecho interno español en la Ley 32/2003, de 3 de noviembre,

Fundación Telefónica
Telefónica

General de Telecomunicaciones, que en su artículo 38.3 indica que: «En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos: […] f) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada. g) A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada»[8].

Si la mera ocultación del número de llamada entrante ha merecido tal atención dentro de la UE como una indudable garantía para el ejercicio de diversos derechos fundamentales, mucho más interés debería tener la protección del anonimato a la hora de navegar por Internet. Como cualquiera puede imaginar, el estudio de una mera relación de páginas visitadas por una persona concreta, sobre todo si el rastreo se refiere a un periodo de tiempo más o menos prolongado, puede ofrecer una enorme información sobre la personalidad, la economía, los gustos, las aficiones o las preocupaciones de ese ciudadano en concreto. El perfil obtenido puede ser utilizado con diversos fines y puede entrañar serias amenazas para su libertad o seguridad.

Antecedentes en la jurisprudencia internacional

De hecho, la jurisprudencia internacional ha tenido ya la oportunidad de pronunciarse sobre estos extremos. Así, el Tribunal Europeo de Derechos Humanos, en su Sentencia de 3 de abril de 2007 (Caso Copland)[9], analizó si el seguimiento de las llamadas telefónicas, del uso del correo electrónico y de la navegación por Internet realizada por los responsables de un *College* universitario de Gales (Reino Unido) sobre una trabajadora del mismo suponía una violación de los derechos reconocidos en el Convenio Europeo de Derechos Humanos. En sus alegaciones, el Gobierno británico aceptó que, en este caso, «si bien se efectuó cierto seguimiento de las llamadas, el correo electrónico y la navegación por Internet de la demandante con anterioridad a noviembre de 1999, no se llegó a interceptar las llamadas telefónicas ni a analizar el contenido de las páginas web visitadas por ella». Para el gobierno inglés, «el seguimiento no consistió, pues, en nada más que en un análisis de la información generada automáticamente para determinar si las instalaciones del *College* se habían usado con fines personales» (STEDH 23/2007, parágrafo 32). Se trataba no de interceptar el contenido de las llamadas o de los correos electrónicos, sino simplemente de conocer a qué números se llamaba, a quién se enviaban los correos electrónicos y el nombre o la dirección de las páginas web que se consultaban. Es más, según sus alegaciones, «En el supuesto de que el análisis de la relación de llamadas telefónicas, el correo electrónico e Internet se considerase una injerencia en el respeto de la vida privada o la correspondencia, el Gobierno señala que la injerencia estaba justificada» (STEDH 23/2007, parágrafo 33), ya que «En primer lugar, perseguía el fin legítimo de proteger los derechos y libertades de los demás al asegurar que no se abusase de unas instalaciones con cargo a los fondos públicos»; y en segundo lugar, «la injerencia tenía un fundamento en derecho interno en la medida en que el *College*, como organismo estatutario, cuyos poderes le facultan para ofrecer formación superior y hacer lo necesario y oportuno con tal propósito, tenía el poder de controlar razonablemente sus instalaciones para asegurar su capacidad de llevar a cabo sus funciones estatutarias». Concluía que «era razonablemente previsible que las instalaciones con las que cuenta un organismo estatutario con cargo a los

Fundación Telefónica
Telefónica

fondos públicos no podían ser utilizadas en exceso con fines personales» ((STEDH 23/2007, parágrafo 34).

A pesar de estas alegaciones, el Tribunal consideró que tales injerencias eran injustificadas, ya que «según la reiterada jurisprudencia del Tribunal, las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de 'vida privada' y de 'correspondencia', a efectos del artículo 8.1 (Sentencias Halford [TEDH 1997, 37], previamente citada, ap. 44 y Amann contra Suiza [TEDH 2000, 87] [GC], No. 27798/1995, ap. 43, TEDH 2000-II). Es lógico pues que los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del artículo 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet»[10].

Asimismo, el Tribunal recuerda que «la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el artículo 8 (RCL 1999, 1190 y 1572), ya que dicha información es «parte de las comunicaciones telefónicas» (Sentencia Malone contra el Reino Unido, de 2 agosto 1984 [TEDH 1984, 1], serie A No. 82, ap. 84)» y el hecho de que el *College* obtuviese esos datos legítimamente, 'en forma de facturas telefónicas', no es impedimento para «constatar una injerencia en los derechos garantizados por el artículo 8 (ibídem)» Y, lo que resulta más relevante, «el almacenamiento de datos personales relativos a la vida privada de una persona se halla también en el ámbito de aplicación del artículo 8.1 (Sentencia Amann [TEDH 2000, 87], previamente citada, ap. 65)» (parágrafo 43). Además, el Tribunal considera que tan injerencia no estaba justificada ni por el derecho interno ni por las normas internacionales (parágrafos 45-48). Por todo ello, «el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio» (parágrafo 44), concediéndole a la recurrente una indemnización por daño moral y obligando al Gobierno británico a correr también con los gastos del proceso.

También recientemente, el 22 de septiembre de 2010 el Tribunal Constitucional alemán ratificó una sentencia del Tribunal Supremo alemán del año 2009, en la que este se refería a que el uso anónimo es inmanente a Internet, a la vez que también consideraba que las opiniones anónimas gozaban de la protección de la libertad de expresión[11].

El tratamiento de las direcciones IP

Relacionado también con la protección de la intimidad, al ser un elemento imprescindible para navegar por Internet, hay que prestar atención al trato legal que poseen las direcciones IP[12]. En este sentido, es alentador que la mayoría de las legislaciones europeas consideren a esta dirección como un dato de carácter personal. De hecho, otorgar protección a los datos personales de cara a su tratamiento informático es algo que viene siendo considerado desde mediados de los años setenta del pasado siglo.

Fundación Telefónica
Telefónica

Así, el Grupo de Trabajo sobre el artículo 29[13], en su Dictamen 4/2007 sobre el concepto de datos personales, indicó que «si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona», ya que actualmente pueden utilizarse otros 'identificadores' para singularizar a alguien. Efectivamente, «los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero». Y por lo que se refiere a Internet, «las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona, es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo y atribuirle determinadas decisiones, puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto». En otras palabras, «la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos»[14].

Y en particular, respecto de las direcciones IP, el Dictamen señala que «el Grupo de trabajo considera a las direcciones IP como datos sobre una persona identificable», ya que, como se indicó ya en el año 2000, «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet, que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva»[15]. Así, es posible que «en muchos casos exista la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como *cookies* con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación». Y ello sobre todo si «el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales»[16].

Ya con anterioridad, la legislación española sobre protección de datos iba por el mismo camino. Así, el artículo 3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se refiere a 'dato de carácter personal' como «cualquier información concerniente a personas físicas identificadas o identificables». Y en desarrollo de la misma, su Reglamento (aprobado por Real Decreto 1720/2007, de 21 de diciembre) define en su artículo 5.f) los datos de carácter personal como «cualquier información numérica, alfabética, gráfica,

Fundación Telefónica
Telefónica

fotográfica, acústica o de cualquier otro tipo concerniente a una personas físicas identificadas o identificables». El apartado o) del citado artículo recoge la definición de 'persona identificable' y considera como tal a «toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social».

Esta definición de dato personal que se realiza en términos tan amplios nos permite incluir sin ningún problema como dato personal a todo el que permita vincular una información personal a una persona, condición que sin muchas complejidades puede predicarse de las direcciones IP; y en cumplimiento de ello han existido algunas resoluciones de la Agencia de Protección de Datos[17]. La protección otorgada a las direcciones IP constituye, por lo tanto, un elemento esencial para mantener el anonimato en la Red.

Desde otro punto de vista, grandes empresas de Internet, como Google, han cuestionado que la dirección IP sea considerada un dato personal. Así, en un encuentro que tuvo lugar en mayo de 2008, defendían que la dirección IP no podía ser un dato personal. Los argumentos más importantes eran que, en el caso de ordenadores compartidos -bibliotecas, *cybercafés*, etc.- la asignación de direcciones IP podía ser compartida también por muchas personas diferentes; y que muchos proveedores de Internet asignaban direcciones IP dinámicas, por lo que varias cuentas diferentes podían usar la misma dirección IP durante el curso de una semana. Asimismo, que en ambientes corporativos, cientos de usuarios podían estar conectados a una única dirección IP de salida[18]; que una dirección IP por si sola no puede asociarse a un individuo ni lo identifica, sino que solo identifica a un equipo informático conectado a una red (de hecho, una variedad de equipos como impresoras, fax, escáneres pueden poseer direcciones IP) o que, en fin, las direcciones IP pueden ser falsificadas o disfrazadas (Less, 2009). En este sentido, señalaban la dificultad que se les plantea a empresas como Google, que recolectan direcciones IP, «para garantizar la seguridad y la calidad de servicios»; la caracterización de estos datos como 'datos personales', tanto a la hora del impacto negativo que tendrían en sus operaciones técnicas como a la hora de cumplir con los requisitos establecidos por las legislaciones nacionales para tratar los datos personales. Esto último, especialmente centrado en dos aspectos: requerir el consentimiento para el tratamiento de estos datos en el caso de usuarios no autenticados -incluyendo la prueba de que el consentimiento ha sido otorgado- y el ejercicio de los derechos de acceso, rectificación y cancelación.

La conservación de datos generados por el usuario

Sin embargo, de modo paradójico, la desconfianza de las autoridades en el uso que por los ciudadanos se pueda estar haciendo de Internet ha hecho que la Unión Europea haya aprobado la Directiva 2006/24/CE, que también modifica la anterior Directiva 2002/58/CE, en la que se establecía la obligación de los proveedores de acceso a Internet de conservar los datos generados en las trasmisiones electrónicas.

Así, en los que podíamos considerar como la exposición de motivos de esta Directiva, se señala que, si bien los artículos 5, 6 y 9 de la anterior Directiva 2002/58/CE establecían como

Fundación Telefónica
Telefónica

obligaciones de los proveedores que los datos obtenidos en las transmisiones a través de Internet deberían borrarse o hacerse anónimos cuando no se necesiten para la transmisión, «salvo los datos necesarios para la facturación o los pagos por interconexión»[19], también se permitía que los Estados miembros limitasen esta obligación, siempre que tales restricciones constituyeran «medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas» (Directiva 2002/58/CE, art. 15, apartado 1).

Varios Estados -entre ellos España[20]– hicieron uso de esa posibilidad, aunque con una gran diversidad en sus legislaciones, cuya corrección e igualación venía obligada, que es lo que pretendía la nueva Directiva del año 2006. Así, aunque «de conformidad con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), toda persona tiene derecho al respeto de su vida privada y de su correspondencia» y ello obliga a que no pueda existir injerencia de la autoridad pública en el ejercicio de este derecho, lo cierto es que esta injerencia podrá realizarse cuando «esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros».

Y para la UE, «dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva». Por consiguiente, «la adopción de un instrumento de conservación de datos que cumpla los requisitos del artículo 8 del CEDH es una medida necesaria» (Directiva 2006/24/CE, parágrafo 9).

No obstante, los datos que se deben conservar son los «generados o tratados como consecuencia de una comunicación o de un servicio de comunicación y no los datos que constituyen el contenido de la información comunicada. Los datos deben conservarse de tal manera que se evite que se conserven más de una vez. Los datos generados o tratados, cuando se presten servicios de comunicaciones electrónicas, se refieren a los datos accesibles». En particular, en lo referente a la conservación de datos relativos a los correos electrónicos y la telefonía por Internet, «la obligación de conservar datos solo puede aplicarse con respecto a los datos de los servicios propios de los proveedores o de los proveedores de redes» (Directiva 2006/24/CE, parágrafo 13).

Para ello, el artículo 1 de la Directiva establece, en su apartado 1, la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar determinados datos generados o tratados por los mismos, «para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro». Y en su apartado 2, que los citados datos son concretamente «los datos de

Fundación Telefónica
Telefónica

tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o al usuario registrado», pero no «se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas» (Directiva 2006/24/CE, art. 1)[21]. El periodo de conservación de tales datos se establece en una horquilla que va desde los seis meses como mínimo a los dos años como máximo (art. 6).

En la ley española que aplica esta Directiva comunitaria, la Ley 25/2007[22], se establece una regulación prácticamente idéntica a la recogida en aquella, estableciendo concretamente que la duración de la conservación de los datos sea de doce meses (Ley 25/2007, art. 5). También señala que los datos deben cederse, previo mandamiento judicial, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a los funcionarios del Servicio de Vigilancia Aduanera y al personal del Centro Nacional de Inteligencia (Ley 25/2007, art. 6).

Conclusiones

En definitiva, podemos considerar que los retos jurídicos que plantea Internet y el conjunto de servicios relacionados con la Red (correo electrónico, foros de noticias, redes sociales, etc.) pueden ser abordados desde dos puntos de vista: desde una interpretación flexible de las tradicionales categorías jurídicas o bien desde la creación de nuevos derechos o instituciones que puedan ordenar y resolver los conflictos que se planteen en estos ámbitos, manteniendo las garantías y los derechos de los ciudadanos.

No obstante, parece claro que estas dos visiones no necesariamente deben ser contrapuestas, sino que pueden comportarse pacíficamente de modo complementario, sobre todo si tenemos en cuenta la dificultad que en el ámbito de los derechos fundamentales y de su reconocimiento constitucional existe una gran resistencia a la reforma de las Constituciones.

Debemos tener en cuenta que, aunque pueda parecer que Internet es un ámbito donde reina la libertad, lo cierto es que puede ser fuertemente controlado. De hecho, no existe Internet sin que empresas -privadas, en su gran mayoría- instalen y mantengan las redes físicas imprescindibles para las interconexiones, así como los ordenadores centrales donde se pueden alojar la información (las proveedoras de Internet o ISP, en sus siglas en inglés) o sin empresas privadas que ofrezcan contenidos o que organicen y mantengan a los buscadores, sin los cuales sería imposible encontrar la información deseada. Además, la capacidad de los ordenadores y de los servidores es tan grande en la actualidad que la obligación de mantener los datos generados en las transmisiones electrónicas de millones de ciudadanos conectados, durante periodos que pueden llegar a los dos años, en la legislación europea, no supone ningún problema técnico.

La Red es por tanto un territorio donde los ciudadanos ejercen su libertad, pero también donde esta puede estar amenazada de manera continua y, en esta ocasión, no solo por los propios poderes públicos, sino especialmente por empresas privadas transnacionales, con intereses económicos concretos, que pueden escapar fácilmente al control de las autoridades, en unos casos, o plegarse fácilmente a sus exigencias, en otros. Ello obliga a un especial cuidado en el

Fundación Telefónica
Telefónica

diseño y uso de los instrumentos de control y de garantía de los derechos de los ciudadanos, de tal modo que el total desarrollo de las posibilidades tecnológicas no contradiga la naturaleza de los Estados democráticos ni el contenido esencial de los derechos fundamentales reconocidos en los textos internacionales y en las Constituciones.

En definitiva, nos encontramos nuevamente con el peligro de que las Constituciones vuelvan a ser las 'hojas de papel' señaladas por Ferdinad Lasalle arrastradas por el viento de los intereses de quienes constituyen los verdaderos 'factores de poder' de esta nueva sociedad virtual (Lasalle, 1984, pp. 123 y ss.). A todos nos compete, bien como ciudadanos o bien como juristas, no abandonar nuestras responsabilidades y, en el ámbito que a cada uno nos corresponda, ejercer responsablemente nuestros derechos y defender su ejercicio. Del éxito que tengamos va a depender nuestra libertad y la naturaleza del modelo de sociedad que se avecina.

Bibliografía

Comisión Europea (2006, 20 de marzo). *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. Superar los desequilibrios de la banda ancha.* Bruselas.

Cotino Hueso, L. (2005). Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los blogs). En VV.AA., *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías.* Burgos: Universidad de Castilla y León, Facultad de Derecho.

De Vergottini, G. (1985). *Derecho Constitucional Comparado.* Madrid: Espasa-Calpe.

Gibson, W. (1985). *Neuromante.* Traducción de José Arconada y Javier Ferreira. Barcelona: Minotauro.

Jellinek, G. (1991). *Reforma y Mutación de la Constitución.* Madrid: Centro de Estudios Constitucionales.

Lasalle, F. (1984). *¿Qué es una Constitución?* Barcelona: Ariel.

Less Andrade, P. (2009, mayo). Google, protegiendo la privacidad en Internet. *VI Encuentro Iberoamericano de Protección de Datos* [en línea]. Cartagena de Indias. Disponible en: *https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/pla_privacidad_internet_vi_encuentro_iberoamerica.pdf* [Consulta: 2009, 28 de agosto].

Murillo Ferrol, F. (1972). *Estudios de sociología política*. Madrid: Tecnos.

Orza Linares, R. M. (2003). *Fundamentos de la democracia constitucional: los valores superiores del ordenamiento jurídico.* Granada: Comares.

Fundación Telefónica
Telefónica

Serrano Pérez, M. M. (2003). *El derecho fundamental a la protección de datos.* Madrid: Civitas.

Notas

1 La novela fue publicada en español en 1985.

2 Definido como «un sistema global de información que: está relacionado lógicamente por un único espacio global de direcciones basado en el protocolo IP [designación de una localización concreta en Internet, normalmente un ordenador, compuesta por un número único compuesto de cuatro partes separadas por puntos] o sus extensiones; es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones y/o otros protocolos compatibles con IP; proporciona, usa o hace accesible, de manera pública o privada, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas». Resolución de 24 de octubre de 1995 del *Federal Networking Council* estadounidense (la referencia original puede consultarse en: *http://www.reference.com/browse/Federal+Networking+Council* [Consulta: 2010, 22 de agosto]). Actualmente este Consejo ha sido sustituido por el *National Science and Technology Council* (véase: *http://www.ostp.gov/cs/nstc* [Consulta: 2010, 22 de agosto]) y el archivo de las resoluciones del FNC puede consultarse en: *http://www.nitrd.gov/archive/fnc-material.html* [Consulta: 2010, 22 de agosto].

3 Voto particular del magistrado Jiménez de Parga, al que se sumó también el magistrado Mendizábal Allende, a la STC 290/2000, de 30 de noviembre (Pleno). Ponente: González Campos. Recursos de Inconstitucionalidad contra la Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal (BOE No. 4, de 4 de enero de 2001, Suplemento, pp. 70-93). El voto particular, a partir de la p. 92.

4 Como ejemplo, la Cumbre Mundial de la Sociedad de la Información, celebrada en Ginebra (primera fase, 2003) y Túnez (segunda fase, 2005). Véase: *http://www.itu.int/wsis/geneva/index-es.html, http://www.itu.int/wsis/tunis/index-es.html* y *http://lac.derechos.apc.org/wsis/index.shtml* [Consulta: 2009, 28 de agosto].

5 En la *Declaración de Derechos del Ciberespacio* que Robert B. Gelman redactó el 12 de noviembre de 1997, en su artículo 3 se establecía que «Toda persona tiene derecho a la privacidad, anonimato y seguridad en las transacciones en línea». Aunque de dudosa eficacia, tiene a su favor el adelantarse a algunos de los problemas que debe afrontar la regulación de Internet. Puede consultarse el texto de la Declaración y un breve análisis de la misma, realizada por Liceli Gabriela Peñarrieta Bedoya, en *Derecho al acceso a las tecnologías de comunicación e información*. Disponible en: *http://www.monografias.com/trabajos37/derechos-ciberespacio/derechos-ciberespacio2.shtml* [Consulta: 2009, 28 de agosto].

6 Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002 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). Disponible en:

Fundación Telefónica

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF [Consulta: 2009, 28 de agosto].

7 Art. 10: « […] el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público podrá anular: […] 2. la supresión de la presentación de la identificación de la línea de origen y el rechazo temporal o la ausencia de consentimiento de un abonado o un usuario para el tratamiento de los datos de localización, de manera selectiva por línea, para las entidades reconocidas por un Estado miembro para atender llamadas de urgencia, incluidos los cuerpos de policía, los servicios de ambulancias y los cuerpos de bomberos, para que puedan responder a tales llamadas».

8 Es significativo que, si bien la Directiva se refiere a las llamadas telefónicas, en la legislación española se extiende este derecho a las 'comunicaciones electrónicas', concepto que parece más amplio que las meras llamadas telefónicas. Toda la legislación española puede consultarse en: *http://www.boe.es/*

9 Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) 23/2007, de 3 de abril. La jurisprudencia del Tribunal, usualmente en francés o inglés, puede consultarse en: *http://www.echr.coe.int/*. La página web del Consejo de Europa es: *http://www.coe.int/*

10 Parágrafo 41. Artículo 8 del Convenio Europeo de Derechos Humanos (4 de noviembre de 1950): «Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

11 La sentencia se refiere a una página web (*http://www.spickmich.de/*) en la que, de forma anónima, se introducían valoraciones sobre profesores. El caso se suscitó a partir de la denuncia de una profesora que fue valorada en esa página (BVerfG, Beschluss von 16-08-2010, Az. 1 BvR 1750/09).

12 Según la *Wikipedia*, una dirección IP es «un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC, que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar. Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar cada vez que se conecta; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica). Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web, necesariamente deben contar con una

Fundación Telefónica
Telefónica

dirección IP fija o estática, ya que de esta forma se permite su localización en la Red. A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio. La traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS. Existe un protocolo para asignar direcciones IP dinámicas, llamado DHCP (*Dynamic Host Configuration Protocol*)». Véase: Colaboradores de Wikipedia. *Dirección IP* (2009) *Wikipedia, La enciclopedia libre* [en línea]. Disponible en: *http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP* [Consulta: 2009, 28 de agosto].

13 Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad y está compuesto por representantes de las autoridades nacionales de control de datos de los Estados miembros, de un representante del Controlador Europeo para la Protección de Datos (CEPD) y de un representante de la Comisión Europea. Como ya hemos indicado, la dirección de Internet en la que se puede consultar toda la legislación europea es *http://eur-lex.europa.eu*.

14 Grupo de Trabajo del artículo 29, Dictamen 4/2007 sobre el concepto de datos personales (20 de junio de 2007). Disponible en: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf*, p. 15 [Consulta: 2009, 28 de agosto].

15 Documento de trabajo *WP 37: Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*, adoptado el 21 de noviembre de 2000, p. 23. Disponible en español en: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37es.pdf* [Consulta: 2009, 28 de agosto de].

16 Ibídem, pp. 18-19.

17 Resolución de la Agencia Española de Protección de Datos de fecha 5 de marzo de 2009. Se trata de una resolución dictada en un procedimiento abierto por una denuncia presentada por el Director de la Oficina de Defensa de los Derechos del Menor de las Islas Baleares, en la que se ponía de manifiesto que una página web en la que existía una red social denominada Tcuento publicaba las direcciones IP de las personas que participaban en la misma, muchos de ellos menores de edad. Este procedimiento no pudo concluir con sanción, por no encontrar a la persona responsable de la citada página web. Hace algunos años, esta Agencia ya defendía que la dirección IP era un dato de carácter personal, obligando al registro en la propia Agencia de las bases de datos que recogieran esos datos, en su Informe 327/2003, *Carácter de dato personal de la dirección IP*. El texto de esta Resolución y de las otras dictadas por esta Agencia, puede encontrarse en su página web (véase: *http://www.agpd.es/*). Para una descripción somera de las características de esta Agencia, Véase Serrano (2003), pp. 471 y ss.

18 En este sentido, es significativo que en la Resolución de fecha 19 de julio de 2006 de la Agencia Española de Protección de Datos se decidiera el archivo de una denuncia por publicación de datos personales, por cuanto la dirección IP de la que provenía la información correspondía a un servidor *proxi* de la Universidad de Alicante, sin que constara que persona

Fundación Telefónica
Telefónica

concreta podría haberla utilizado. El texto completo de la Resolución se puede consultar en: *https://www.agpd.es/portalweb/resoluciones/archivo_actuaciones/archivo_actuaciones_2006/common/pdfs/E-01055-2005_Resolucion-de-fecha-19-07-2006_Art-ii-culo-6-LOPD.pdf* [Consulta: 2009, 28 de agosto].

19 Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que modifica la anterior Directiva 2002/58/CE. Parágrafo 3. Disponible en: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF* [Consulta: 2009, 28 de agosto].

20 En la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.

21 Concretamente, en el artículo 5 se pormenorizan los datos que necesitan ser conservados. Además, en el apartado 2 de dicho artículo 5 se enfatiza de nuevo que «De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación».

22 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE No. 251, de 19 de octubre de 2007).

Fundación Telefónica
Telefónica