

MONOGRÁFICO

VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet

 Miquel Peguera Poch (coord.)

Sumario

1. Presentación, por Miquel Peguera Poch.....	22
2. Neutralidad de la Red: Historia, regulación y futuro, por Christopher T. Marsden	24
3. El concepto de <i>net neutrality</i> y la tensión entre regulación pública y autorregulación privada de las redes, por Joan Barata Mir	44
4. Privacidad en Internet y el derecho a ser olvidado/derecho al olvido, por Cécile de Terwangne	53
5. El olvido: El derecho a ser diferente... de uno mismo Una reconsideración del derecho a ser olvidado, por Norberto Nuno Gomes de Andrade	67
6. Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido, por Javier de la Cueva González-Cotera	84

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet?»

Presentación

La neutralidad de la Red, o *net neutrality*, así como el llamado «derecho al olvido» en Internet, son sin duda dos de los temas más acuciantes en el actual debate sobre el futuro de Internet. Las dos materias presentan perfiles complejos y suscitan posturas contrapuestas, con puntos de vista muy diversos, tanto de los actores directamente implicados como de los académicos, reguladores, y de la comunidad de usuarios en general. La discusión alcanza tanto al sentido y límites de estos principios, como al papel que, en su caso, debería desempeñar el legislador para garantizar su efectividad.

La idea básica que subyace en la noción de neutralidad de la Red es el objetivo de que las redes de telecomunicaciones actúen como vehículos neutrales en la transmisión de los datos, de tal modo que no tenga lugar discriminación alguna en razón del origen de la información, de su naturaleza o de las aplicaciones a las que los usuarios desean acceder. En buena medida esta neutralidad ha sido consustancial al diseño primigenio de Internet y puede quedar en entredicho ante determinadas prácticas de gestión del tráfico que priorizan la transmisión de los datos en atención a sus características o en función de las distintas fórmulas de contratar los servicios, estableciendo niveles diversos de calidad. Algunas de estas prácticas pueden poner en riesgo no sólo la libertad de expresión y de información, sino el propio desarrollo tecnológico de la Red y la aparición de nuevas aplicaciones. A la vez suscitan interrogantes desde el punto de vista del derecho de defensa de la competencia, ya que pueden dar lugar a barreras anticompetitivas para proveedores de contenidos y aplicaciones. Parte de la discusión se centra en si el respeto a estos principios debe dejarse al juego de la libre competencia entre los operadores o si es precisa una intervención legislativa o regulatoria para establecer deberes específicos de neutralidad, y si resultan suficientes en este sentido las previsiones incluidas tras la reforma llevada a cabo en el 2009 en las directivas que conforman el llamado paquete de telecomunicaciones.

Por otra parte, en el debate sobre el llamado «derecho al olvido» se plantea el problema de lograr un equilibrio razonable entre, por una parte, el derecho a la privacidad y la protección de los datos personales, y por otra parte, la libertad de información y de expresión, así como la propia libertad de prestar servicios de búsqueda, agregación y localización de contenidos en Internet. El vertiginoso desarrollo de las capacidades de indexación y búsqueda plantea problemas nuevos en el campo de la privacidad, no sólo en relación con posibles informaciones falsas o difamatorias, sino, sobre todo, por la visibilidad que obtienen determinados datos del pasado, con una proyección que puede perjudicar gravemente las expectativas de las personas en los campos del honor y de la intimidad personal y familiar. También aquí existe un debate abierto sobre si la aspiración a verse libre del pasado debe reconocerse, y en qué términos, como un derecho exigible a los prestadores de servicios de Internet. Se trata de una cuestión muy presente en la agenda de la UE, que se ha plasmado ya en el artículo 17 de la Propuesta de Reglamento General de Protección de Datos presentada a finales de enero del 2012 por la Comisión (Bruselas 25.1.2012; COM[2012] 11 final).

Ambas cuestiones, neutralidad de la Red y derecho al olvido, estuvieron presentes como ejes centrales en el 7.º Congreso Internacional Internet, Derecho y Política (IDP 2011). El monográfico que presentamos en este número de la revista *IDP* recoge algunas de las intervenciones de los ponentes invitados que abordaron de modo específico dichas materias. Hemos incluido dos textos referidos a la neutralidad de la Red, dos artículos que tratan sobre el derecho al olvido y por último, un artículo recapitulativo, en el que el relator del congreso da cuenta de los principales temas que se trataron a lo largo de las dos jornadas de debate y discusión. No ha sido posible incluir aquí todas las ponencias presentadas en las diversas mesas redondas, algunas de las cuales aparecerán en próximos números de la revista. Por otra parte y al margen de las ponencias de los conferenciantes invitados, todo el conjunto de comunicaciones enviadas y

presentadas en el Congreso fueron ya publicadas en las actas del mismo, disponibles en <http://edcp.uoc.edu/symposia/idp2011/proceedings/>

El primero de los textos referidos a la neutralidad de la Red que recoge este monográfico es la conferencia inaugural del Congreso, impartida por el profesor Christopher T. Marsden, que se publica tanto en su versión original inglesa como en español. Bajo el título de «Neutralidad de la Red: Historia, regulación y futuro», la conferencia ofrece un panorama general del estado de la cuestión y de los diversos desarrollos legislativos y sistemas de corregulación en el plano comparado, así como las perspectivas de futuro. El segundo texto es la ponencia del profesor Joan Barata Mir: «El concepto de *net neutrality* y la tensión entre regulación pública y autorregulación privada de las redes». En él se examinan los diversos significados que se atribuyen a la noción de *net neutrality* y se plantean las posibilidades, dificultades y límites de una posible intervención regulatoria ante la falta de incentivos de los ISP para aplicar criterios de neutralidad en la gestión de las redes.

En el ámbito del denominado derecho al olvido, publicamos en primer lugar la conferencia dictada por la profesora Cécile de Terwangne «Privacidad en Internet y el derecho a ser olvidado/derecho al olvido», en la versión original inglesa y la versión traducida al español. A partir de la noción de privacidad en Internet, el texto aborda las diversas manifestaciones del derecho al olvido, incluida su versión más debatida, que supondría la fijación de una fecha de caducidad a los datos personales en el ámbito digital, destacando las dificultades que ello comportaría tanto para su aplicación práctica, como desde el punto de vista del conflicto con otros derechos e intereses legítimos. A continuación, la ponencia de Norberto Nuno Gomes de Andrade, «El olvido: El derecho a ser diferente... de uno mismo. Una reconsideración del derecho a ser olvidado» (de la que también se publica la versión original en inglés) conceptualiza y propone un derecho al olvido basado en el derecho a la identidad.

Por último, el artículo de Javier de la Cueva, relator oficial del Congreso, nos ofrece una visión de conjunto de las principales discusiones y materias tratadas en los dos intensos días de ponencias, comunicaciones y debates.

Miquel Peguera Poch
 Profesor agregado de *Derecho Mercantil* de la UOC
 Coordinador del monográfico

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet»

ARTÍCULO

Neutralidad de la Red: Historia, regulación y futuro

Christopher T. Marsden

Fecha de presentación: junio 2011

Fecha de aceptación: julio 2011

Fecha de publicación: febrero 2012

Resumen

Este artículo se centra en el reto de política global de la neutralidad en la red: ¿Podrán los gobiernos garantizar un acceso creciente a un Internet aún más rápido, y a la vez defender las expectativas de los usuarios y los proveedores de contenidos de que la censura y el filtrado de sus contenidos se mantendrán en los mínimos democrática y económicamente necesarios? ¿O bien el acceso al Internet abierto se relegará a un carril comparativamente lento, con carriles rápidos reservados para servicios preferentes de vídeo, telefonía y otros, afiliados a los proveedores de servicios de acceso a Internet? La regulación de las comunicaciones de telefonía, radiodifusión e Internet (incluido el comercio electrónico) depende de las soluciones a estas preguntas, agrupadas en el principio, convertido en slogan, de *neutralidad de la red*.

Palabras clave

neutralidad de la red, Internet, investigación, políticas

Tema

Derecho

Network Neutrality: History, Regulation and Future

Abstract

This article focuses on the global policy challenge of network neutrality. Will governments be able to ensure increasing access to an ever faster Internet while supporting user and content provider expectations that censorship and filtering of their content is kept to a democratically and economically necessary minimum? Or will open Internet access be relegated to a comparatively slow lane, with fast lanes reserved for ISPs' affiliated video, telephony and other preferred services? Communications regulation of telephony, broadcasting and the Internet (including consumer electronic commerce) depends on the solutions found to these questions, grouped in the sloganised principle of 'network neutrality'.

Keywords*network neutrality, Internet, research, policy***Topic**

Law

1. Historia: el protocolo *trust-to-trust* y el control de las comunicaciones

La neutralidad en la red es la última fase de una eterna discusión sobre el control de los medios de comunicación. Los primeros analistas jurídicos y técnicos sostenían que Internet era especial, debido a su construcción descentralizada, que lo distinguía de las anteriores tecnologías de la libertad (de Sola Pool, 1983), como la radio y el telégrafo. Spar (2001) sostiene que el control es un paso evolutivo histórico en el desarrollo de los medios de comunicación, mientras que Wu (2010), siguiendo a Lessig (1999), argumenta que la clausura no tiene por qué ser un resultado inevitable.

Internet nunca había sido objeto de regulación más allá de la necesaria para la interoperabilidad y la competencia, basada en la *First Computer Inquiry* y en la *Second Computer Inquiry* de la Comisión Federal de Comunicaciones (FCC) de Estados Unidos (Werbach, 2005) y en el principio de diseño de extremo a extremo (*end-to-end* [E2E]), que fue descrito por primera vez por Saltzer, Reed y Clark (1984). Ese principio fue superado por la necesidad de una mayor confianza y seguridad en la emergente red de banda ancha a finales de 1990, sobre todo cuando el correo electrónico basura propició la aparición de virus, *botnets* y otros riesgos. Como resultado, E2E ha ido dando paso gradualmente a mecanismos *trust-to-trust*, en los que la recepción del mensaje por el agente de confianza de una de las partes sustituye la recepción por el receptor final (Clark/Blumenthal, 2011). Este agente es casi siempre el proveedor de servicios de Internet (ISP) y es su regulación lo que está en juego en la neutralidad en la red. Los ISP no solo eliminan los mensajes basura y otros materiales peligrosos antes de que lleguen a los suscriptores (que son en general técnicamente legos), también pueden eliminar otros materiales potencialmente ilegales en interés de los gobiernos y los titulares de derechos de autor, por nombrar a dos de los censores más activos en Internet, así como priorizar paquetes en bene-

ficio propio. En consecuencia, el principio E2E se vería amenazado si no estuviera ya moribundo.

Benkler, a quien preocupaba la necesidad de mantener la interoperabilidad y la apertura para garantizar un patrimonio común (*commons*) en el que la innovación no afiliada y no comercial pudiera florecer, entendió muy bien las implicaciones legales y políticas de la rápidamente estandarizada innovación en la ecología de las comunicaciones (Benkler, 1998a, 1998b). Los valores centrales de apertura y democracia de Internet se han establecido tanto por accidente como por diseño. Noam (2008) afirma: «No hay nada especialmente nuevo en la reciente ronda [del derecho de los medios de comunicación] -la neutralidad en la red- ni como cuestión conceptual ni en términos de opciones políticas, salvo en cuanto a la terminología». Benkler (1998) y Lemley y McGowan (1998) han argumentado que, a pesar de que los efectos de red pueden tender a la clausura de la red, el control legal puede no ser el único resultado que traduzca en una mayor apertura.

No es novedoso afirmar que los protocolos regulan el comportamiento del usuario en Internet («el código es ley», como declaró Lessig [1999a]), pero el compromiso legal con la libertad de expresión significa que el derecho puede regular Internet, exigiendo la observancia de las condiciones que permiten la libertad de expresión. Como Wu (2003) explica, tan seguro es que las leyes pueden regular Internet como viceversa; y las leyes pueden hacerlo con más autoridad constitucional aunque con menor habilidad tecnológica (Mayer-Schonberger, 2008; Reidenberg, 2005). En 1998, el debate innovación-control giraba en torno al aprovechamiento por Microsoft de su monopolio en sistemas operativos para el navegador y el software de vídeo, y en 2000 había llevado a examinar a AOL-Time Warner, en particular la posibilidad de controlar la mensajería instantánea y el vídeo (Faulhaber, 2002), y la fusión horizontal de la telefonía por cable, como la de AT&T y MediaOne (Lemley y Lessig, 1999). De aquí se pasó al control sobre wi-fi, una tecnología

de espectro sin licencia, capaz de ofrecer conectividad de red de área local y liberar el control sobre los usuarios finales que ejercían los proveedores de servicios de Internet con conexiones fijas e inalámbricas (Croxford y Marsden, 2001). La expresión *net neutrality* (neutralidad de la red) como descripción se usó por primera vez en el debate sobre las prácticas de gestión del tráfico de Internet (ITMP) o calidad del servicio (QoS) en Internet en 2003 (Lessig y Wu, 2003; Wu, 2003b), aunque el debate se inició cuando los académicos temieron que el modelo de empresa cerrada de la televisión por cable conquistase el Internet abierto en 1999 (Lemley y Lessig, 1999; Lessig 1999a, 1999b).

El tratamiento inicial de la neutralidad en la red trataba de garantizar cuatro «libertades de Internet» (FCC, 2005) a los usuarios finales: libertad para conectar dispositivos, para ejecutar aplicaciones, para recibir los paquetes de contenido que se desee y para obtener «información relevante (...) del Plan de Servicio» (sobre esto último, véase la sección sobre transparencia). Todavía en 2011, algunos académicos sugieren que la libertad de innovar puede ser compatible con prohibiciones de diseño (van Schewick, 2010), a pesar de que los ISP llevan más de una década gastando miles de millones de dólares en el desarrollo de protocolos que les han permitido controlar el tráfico que llega a sus redes (Waclawsky, 2005) y el racionamiento al por mayor del tráfico al usuario final. Berners Lee (2006) declaró: «Se ha sugerido que no necesitamos legislación porque no la hemos tenido hasta ahora. Son tonterías, porque de hecho hemos tenido neutralidad de la red en el pasado; las amenazas explícitas reales se han producido solo recientemente.» Berners Lee fue especialmente firme en que no quiere ver prohibida la calidad de servicio (QoS) porque eso es precisamente lo que reclaman algunos defensores de la neutralidad de la red en Estados Unidos -y a lo que se oponen la comunidad de ingenieros de Internet.

1.1. Historia: definición y desarrollo

Se puede considerar que la neutralidad de la red comprende dos compromisos de no discriminación diferentes (Marsden, 2010a), uno de servicio universal y otro de servicio público de transporte (*common carriage*).

El primero es la llamada «neutralidad de la red *lite*», que mira hacia el pasado y que reivindica que los usuarios de Internet no deberían estar en desventaja por las prácticas opacas y odiosas de sus actuales proveedores de Internet

-las compañías que proveen conexión a Internet en sus hogares. El argumento es que se debe prestar un nivel mínimo de servicio que ofrezca acceso abierto a Internet sin bloquear o degradar aplicaciones o protocolos específicos, lo que se ha descrito como una versión actualizada del servicio universal (Mueller, 1998) y que en general se propone a 2 Mbps. Esto proporciona un nivel básico de servicio que en último término todos los abonados deberían recibir.

En cambio, la llamada «neutralidad de la red positiva», con vistas al futuro, describe una práctica según la cual la oferta de una mayor calidad de servicio (QoS) a precios más altos debe realizarse en condiciones justas, razonables y no discriminatorias (*fair reasonable and non-discriminatory*, FRAND) a todos los interesados, lo que supone un equivalente moderno del servicio público o *common carriage* (Noam, 1994). Se trata de un principio más discutible, y muchos proveedores de contenido y operadores prefieren acuerdos exclusivos. El tipo de servicio que podría acogerse al trato justo, razonable y no discriminatorio podría dar lugar a una exclusividad a corto plazo en sí mismo, ya que es posible, por ejemplo, que las torres de telefonía celular inalámbrica/móvil solo sean capaces de transportar una única transmisión de vídeo de alta definición en un momento dado y por lo tanto pueda producirse un monopolio. Como el principio de servicio público o *common carriage* dicta los términos pero no las condiciones específicas del mercado, la transparencia y la no discriminación no se traducirían automáticamente en una pluralidad de servicios. Estoy en contra de las justificaciones sociales o económicas para prohibir por completo todo tráfico propietario de alta velocidad o para apoyar las versiones estrictas de neutralidad de la red que no permitirían ninguna priorización de tráfico. Hay demasiado en juego, ya sea para esperar que el gobierno suplante al mercado en el suministro de conexiones de mayor velocidad o para que el mercado siga ofreciendo una apertura sin los topes reglamentarios y de política más básicos para asegurar cierto crecimiento (Meisel, 2010, pág. 20).

El problema de neutralidad de la red es complejo y tiene implicaciones de largo alcance: los intentos de despacharlo como un problema que se puede superar con la competencia de las operadoras de telecomunicaciones en el bucle local de abonado (la última milla) (Cave *et al.*, 2009; Renda, 2008) no advierten plenamente los persistentes problemas de fallo de mercado. El servicio físico de Internet a los consumidores está sujeto a una amplia gama de cuellos de botella, no solo en la última milla de conexión al usuario final. Hay poca competencia en la red de retorno (*backhaul*) en los mercados de

ISP fijos, incluso en Europa, donde se mantiene el compromiso a favor de la regulación de la competencia, ya que la red de retorno al por mayor la provee el operador de telecomunicaciones nacional privatizado (*incumbent*) (en el Reino Unido, British Telecom). Incluso si las plataformas compitieran realmente, por ejemplo en los países con amplias infraestructuras de cable, seguiría habiendo problemas de mercado, ya que no hay una necesaria relación directa (ni siquiera extracontractual) entre los proveedores de aplicaciones innovadoras y los ISP (Economides y Tåg, 2007), de modo que las plataformas pueden establecer reglas para «gravar» los paquetes de datos que a la larga empobrecen la cadena de valor de la innovación abierta y que, en última instancia, dañan a los consumidores. Así, las típicas empresas innovadoras, como Facebook (fundada en 2003) y YouTube (fundada en 2005) hubieran tenido menos oportunidad para difundirse de forma viral por Internet, ya que sus servicios habrían estado sujetos a estos costes adicionales. Muchos proveedores de contenidos comerciales, como Google, usan redes de distribución de contenidos (*content delivery networks*) y otros mecanismos de almacenamiento en caché para acelerar la velocidad de entrega a los usuarios, reduciendo así el número de *routers* por los que deben pasar los paquetes de datos. El contenido, por tanto, ya se sirve a diferentes velocidades dependiendo de la prioridad de pago que el proveedor de contenido le asigna, y no de las políticas de los ISP.

1.2. Historia: cómo la gestión del tráfico ha cambiado el servicio público de transporte (*common carriage*)

La congestión de la red y la falta de ancho de banda en horas punta es una característica de Internet. Siempre ha existido. Por eso, hasta finales de la década de 1990, el vídeo por Internet era simplemente inviable. Es la razón por la que los servicios de voz por Internet tienen una calidad desigual y también la razón de que los ingenieros hayan estado tratando de crear una mayor calidad de servicio (QoS). El paradigma *end-to-end* (extremo a extremo) es un arma de doble filo, que ofrece las ventajas de una red abierta y «tonta», pero también las desventajas de la congestión, de la fluctuación y, en último término, una tasa decreciente de progreso para las aplicaciones finales de gama alta como el vídeo de alta definición. Puede tener desventajas para quienes optan por la zonificación, en comparación con la provisión de “calidad de servicio” y en este sentido tiene un claro paralelismo con el servicio público de transporte (*common carriage*). Los operadores del servicio público de transporte (*common*

carriers), que por una parte reclaman los beneficios de derechos de paso y otros privilegios, pero por otra exigen controlar el tráfico para obtener mayores beneficios y no por motivos de integridad de la red, tratan de conseguir lo mejor de ambos mundos (Frieden, 2010b). Es conveniente señalar qué no es servicio público de transporte (*common carriage*). No es una tarifa plana para todos los paquetes. Tampoco es necesariamente una tarifa plana para todos los paquetes de un tamaño determinado. Es, en cambio, un acuerdo medieval de no discriminación, entre el soberano y la red de transporte o equipamiento donde tiene lugar el intercambio: al ser calificados como *common carriers*, se otorgan a estos actores privados determinados derechos y beneficios de los que carecerán los transportistas privados ordinarios. Como ha escrito Cherry (2006), los *common carriers* no son una solución a un problema de competencia, son muy anteriores al derecho de la competencia. Impiden la discriminación cuando se trata del mismo tipo de tráfico. Así, si yo le ofrezco a usted el transporte de su transmisión de vídeo de alta definición de un determinado protocolo, el próximo cliente me podrá exigir lo mismo, sujeto a la capacidad, si Internet tuviera que regirse por principios de servicio público o *common carriage*.

La nueva tecnología permite a cualquiera de los *routers* del ISP, si están debidamente equipados, mirar dentro de un paquete de datos para ver su contenido mediante lo que se conoce como inspección profunda de paquetes (*deep packet inspection*, DPI) y otras técnicas. Los *routers* antiguos no eran capaces de realizar más que una inspección superficial, que tan solo permitía determinar la información de cabecera, el equivalente a la dirección postal del paquete. Un ISP puede usar la DPI para determinar si un paquete de datos necesita un transporte de alta velocidad -como en el caso de una transmisión de televisión, que requiere un canal de transmisión dedicado- y puede ofrecer una capacidad dedicada de más velocidad a ese contenido, típicamente contenido que requiere transmisión en tiempo real, como la televisión, películas o llamadas telefónicas que usan VoIP. La mayoría de las llamadas de voz y de vídeo hoy en día usan una línea dedicada, su línea telefónica de cobre o su línea de cable: mañana podrían usar carriles de alta velocidad dedicados en su conexión a Internet. Esto podría ser un buen negocio para los ISP que deseen ofrecer mayor capacidad usando DPI (no todos los ISP lo harán y es bien posible gestionar el tráfico de forma menos intrusiva mediante el protocolo DiffServ para priorizar flujos de tráfico dentro del mismo canal de Internet). Waclawsky (2005) declaró: «Esta es la opinión de consenso emergente: [esto] permitirá a los

proveedores de banda ancha y a los operadores poner una capa de control y una caja registradora en Internet y cobrar por ello de forma creativa».

La DPI y otras técnicas que permiten a los ISP priorizar contenido también les permiten reducir la velocidad de otros contenidos, así como acelerar este para quienes pagan (y para las comunicaciones de emergencia y otros paquetes «buenos»). Esto puede amenazar el negocio de las empresas que compiten con ese contenido: Skype ofrece VoIP con velocidad de Internet normal; uTorrent y el iPlayer de la BBC ofrecen vídeo con protocolos *peer-to-peer* (P2P). La encriptación es habitual en estas aplicaciones y logra en parte esquivar estos controles de los ISP, pero aunque todos los usuarios y aplicaciones usaran un cifrado fuerte, no lograrían superar las decisiones de los ISP de enrutar el tráfico *premium* a un carril más rápido, consignando todo el resto del tráfico a un carril no prioritario más lento (una explicación política que simplificaría una compleja decisión de ingeniería). Los protocolos P2P están diseñados para hacer un uso más eficiente de las redes congestionadas y sus defensores afirman que con la implementación suficiente, los protocolos P2P podrían superar en gran medida los problemas de congestión.

Las técnicas de gestión del tráfico no solo afectan al contenido de alta velocidad y grandes beneficios, sino también, por extensión, al resto del contenido. Solo se puede construir un carril de alta velocidad en una autopista creando desigualdad y con frecuencia las obras de mejora ralentizan a todos los que usan las carreteras en ese momento. Internet puede ser diferente, ya que los reguladores y los usuarios pueden tolerar mucha más discriminación en beneficio de la innovación. Para tomar esta decisión con conocimiento de causa, es de interés público investigar de manera transparente tanto la *net neutrality lite* (los carriles lentos) como la *net neutrality heavy* (qué reglas permiten contenidos a mayor velocidad). Por ejemplo, en ausencia de supervisión, los ISP podrían usar la DPI para bloquear algún contenido por completo, si deciden que no beneficia a los ISP, a los titulares de derechos de autor, a los padres o al gobierno. El bloqueo por parte de los ISP está ya muy extendido con el control del *spam* y, en algunos países, con el bloqueo de imágenes de contenido sexual ilegal.

Uno de los principales argumentos de los ISP que desean gestionar el tráfico de Internet es que no es posible manejar el crecimiento del tráfico con los medios tradicionales de ampliación del ancho de banda y que, por tanto, sus prácti-

cas son razonables. Con el fin de analizar adecuadamente este argumento, los reguladores deben tener acceso a los datos de medición de tráfico de los ISP. Hay varios medios posibles de acceder a los datos en los puntos de intercambio de Internet, pero muchos datos son privados, ya sea porque se trata de transmisiones entre pares (*peers*) que no usan un punto de intercambio o porque se transmiten por una red de distribución de contenidos (CDN). Ningún regulador gubernamental ha producido datos fiables, y los datos propios de las operadoras y de las redes de distribución de contenidos están protegidos por la confidencialidad comercial (por ejemplo, la red propietaria de distribución de contenidos de Google). En junio de 2009, las pruebas de evaluación comparativa EpiTiro mostraron que la banda ancha del Reino Unido funciona a 0,9 Mbps en la hora punta del final del día, un nivel inferior al que se requiere para la transmisión de vídeo del iPlayer de la BBC. Las demoras en la red también la hacen poco fiable para los videojuegos o los servicios de VoIP (ThinkBroadband, 2009): «los usuarios recibieron un promedio del 24% de la velocidad máxima anunciada (...) Durante las horas punta (de las 6 de la tarde hasta la medianoche), la velocidad se redujo en aproximadamente un 20% (...) Los tiempos de *ping*, una medida importante para los juegos *online*, fueron de alrededor de 150 ms, que es un tiempo demasiado alto para un rendimiento de juego aceptable».

2. Regulación: el régimen legal de la neutralidad de la red

Aunque desde 2003, en la Comisión Federal de Comunicaciones (FCC) la neutralidad de la red fue tema de discusiones sobre regulación, y de establecimiento de condiciones en las fusiones (Frieden, 2010b, 2011), su *status* resultaba incierto a mediados de 2011; el Congreso no había aprobado legislación al respecto y las acciones de la FCC se limitaron a casos aislados de discriminación que llegaron a juicio (*Comcast v. FCC*, 2010). El presidente Obama llegó al poder con el compromiso de legislar sobre la neutralidad de la red (Marsden, 2010a: 1). La FCC, mediante una comunicación de propuesta de regulación (*notice of proposed rulemaking* [NPRM]) realizó una consulta pública sobre la neutralidad de la red en 2009/10. Justo cuando este proceso estaba terminando, en abril de 2010, el Tribunal de Apelación (*Comcast v. FCC*, 2010) consideró que las acciones regulatorias de la FCC en este campo no hallaban justificación en la Ley de Telecomunicaciones de 1996 (Ammori, 2010). El éxito de la apelación de Comcast significó que la FCC tenía tres opciones legales:

recuperar la autoridad de servicio público del Título II para los ISP bajo la Ley de Telecomunicaciones de 1996, pedir al Congreso que volviera a legislar para conferirle autoridad del Título I, o tratar de imponer su propia autoridad de Título I, sujeta a impugnación judicial (Marsden, 2010a). Adoptó esta última opción en su orden de 23 de diciembre de 2010 (FCC 2010), que ha de ser impugnada ante los tribunales (Frieden, 2011, pág. 6-15). Esta suspensión de la actividad reguladora puede dejar a la FCC en suspenso durante gran parte de 2012 y los investigadores deben dirigirse a otras instancias en relación con la regulación de la neutralidad de la red (Marsden, 2010b; Meisel, 2010, Donahue, 2010).

A finales de 2009, las instituciones europeas acordaron imponer condiciones de transparencia y de *net neutrality lite* a los ISP, en las Directivas que tenían que haber sido transpuestas a las legislaciones nacionales antes de mayo de 2011. El Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) (2010) señala que las disposiciones legales de las Directivas permiten una regulación más «simétrica» de todos los operadores, no solo de los operadores dominantes, pero pide aclaraciones sobre estas medidas: El artículo 5.1 de la Directiva de Acceso ahora menciona explícitamente que las autoridades nacionales de regulación pueden imponer obligaciones «a las empresas que controlen el acceso a los usuarios para que sus servicios sean interoperables». Se puede usar el nuevo y más amplio ámbito para la resolución de conflictos de interoperabilidad:

«el artículo 20 de la directiva marco ahora prevé la resolución de conflictos entre empresas que suministran redes o servicios de comunicaciones electrónicas y también entre esas empresas y otras que se benefician de obligaciones de acceso y/o interconexión (con la definición de acceso también modificada en el artículo 2 de la Directiva de Acceso como se ha mencionado anteriormente). Las resoluciones de conflictos no pueden ser consideradas como herramientas sencillas para el desarrollo de una política regulatoria, pero sí ofrecen la opción de hacer frente a algunas situaciones específicas (tal vez urgentes). El posible resultado de los conflictos basados en las obligaciones de transparencia pueden suponer una amenaza creíble a las empresas para que cumplan esas obligaciones, ya que su vulneración puede desencadenar la imposición de requisitos mínimos de calidad a una empresa, de acuerdo con el artículo 22 (3) de la Directiva de Servicio Universal.»

En 2011, la Comisión Europea está llevando a cabo consultas sobre el futuro de la obligación de servicio universal

(Comisión Europea, 2010a) que se puede ampliar a una banda ancha de 2 Mbps (afectando al derecho de los Estados miembros en 2012), lo que significará un nuevo umbral de niveles de servicio mínimo en Europa. También requerirá compromisos de ofrecer ese nivel de acceso en el Internet abierto y no una red limitada, bloqueada o cerrada.

2.1. Las respuestas legislativas nacionales

La neutralidad de la red se ha llevado a la legislación o regulación con mayor eficacia en Japón y en la Unión Europea, así como en Noruega y Canadá (donde recibe el nombre de *Internet traffic management practice* [ITMP]: De Beer, 2009). Noruega, Estado miembro del Espacio Económico Europeo (sin participación completa en la UE), trató la neutralidad de la red en 2008-9. La denuncia surgió por primera vez debido a un conflicto entre un ISP, NextGenTel, y la cadena estatal de radiodifusión NRK de Noruega a mediados de 2006 (Marsden, 2010a, pág. 172-173). El regulador noruego convenció a los ISP y las compañías de cable para que firmasen un pacto de corrección sobre transparencia y derechos de los consumidores en 2009. El código noruego (2009) establece que:

- se debe dar a los usuarios información completa y precisa sobre el servicio que están comprando, en particular sobre la capacidad y la calidad;
- los usuarios pueden enviar y recibir el contenido que deseen, usar los servicios y aplicaciones de su elección y conectar cualquier *hardware* y *software* que no dañe la red; y
- la conexión no puede ser objeto de discriminación basada en la aplicación, el servicio, el contenido, el remitente o el destinatario.

A nivel nacional, los Estados miembros de la UE han sido lentos en reconocer los problemas de neutralidad de la red, a pesar de los fuertes indicios anecdóticos que han aparecido (Dunstone, 2006). Ofcom, la autoridad regulatoria sobre las telecomunicaciones del Reino Unido, se ha limitado a medir el rendimiento de la banda ancha de los ISP y a facilitar a los consumidores el cambio a proveedores rivales (Kiedrowski, 2007). El propio Gobierno se ha mostrado indolente y ha llegado a informar erróneamente a la Comisión Europea, en su *15º Informe anual de aplicación de liberalización de las telecomunicaciones*, de que no se estaban produciendo problemas.

En los Países Bajos, en junio de 2011, se presentó una disposición sobre neutralidad de la red en el parlamento, a raíz de la controversia sobre la intención de KPN Mobile de cobrar adicionalmente por servicios de VoIP y mensajería de texto de otros proveedores. La votación fue pospuesta en dos ocasiones, los días 14 y 21 de junio, y seguía pendiente al tiempo de finalizar este artículo.

La neutralidad de la red resulta políticamente controvertida en Canadá, donde tuvo lugar una famosa infracción en 2005 (De Beer, 2009). La autoridad regulatoria anunció una investigación basada en pruebas de infracción de neutralidad de la red en 2009. Como resultado, se declararon nuevos principios de transparencia y no discriminación; estos principios están a la espera de casos y decisiones regulatorias que añadan detalle a las declaraciones generales.

2.1.1. Los topes del ancho de banda

La facturación por uso (UBB, *usage-based billing*), por usar la expresión canadiense, no es nueva en la política de Internet. Era el sistema por defecto en la mayoría de los países antes de la introducción de los módems de banda ancha a finales de los noventa. Solo en los países con tarifa plana de llamadas locales, como Canadá y Estados Unidos, la conexión de Internet tenía una tarifa plana (Oftel, 2000). La facturación por uso pasó a ser un tema de titulares de prensa en el año 2010 en Estados Unidos y Canadá. Geist (2011) ha identificado diferentes prácticas. Con la introducción de cable de banda ancha en Canadá, el regulador nacional, la Comisión Canadiense de Radio, Televisión y Telecomunicaciones (CRTC), permitió la facturación por uso con topes de descarga mensual para los usuarios. Se justificó por el recurso compartido usado por los suscriptores de módem por cable en el bucle local. La CRTC (2011) reiteró su permiso para la facturación por uso, justificada en función de sus atribuciones para garantizar la competencia en virtud del artículo 7 de la Ley de Telecomunicaciones de 1993. Comcast, en Estados Unidos, creó un tope de 250 GB (Burstein, 2008), lo que se consideró más transparente que su anterior recurso a técnicas de DPI y a otras técnicas aplicadas por su subcontratista Sandvine para impedir los intercambios de archivos con protocolos *peer-to-peer*.

En la mayor parte de los casos, la facturación por uso se refiere a la capacidad máxima de descarga y se evalúa de forma independiente de las velocidades de descarga máxima que pueden recibir los usuarios, que son las que general-

mente se publicitan en los anuncios sobre banda ancha dirigidos a los consumidores. La OCDE (2008) muestra que de 215 paquetes de banda ancha tomados como muestra, casi la mitad daría lugar a que los usuarios superaran sus límites mensuales en tres horas a las velocidades máximas anunciadas. La OCDE (2010) muestra que mientras que dos países (Japón y Corea del Sur) han reemplazado casi la mitad de sus líneas de cobre con fibra óptica, la gran mayoría siguen siendo líneas de cobre. Hay una amplia variación en las prácticas entre países, aunque las comparaciones son difíciles de poner en contexto (Bauer, 2010). Australia y Nueva Zelanda, que estaban en la parte inferior de las tablas de la OCDE en la oferta de ancho de banda en 2008, han adoptado la medida radical de encargar la instalación de bucle local de fibra para reemplazar el monopolio de telefonía del operador dominante. La intervención pública no es en modo alguno un tabú en la inversión en banda ancha, y la Comisión Europea ha aprobado repetidamente todas las inversiones públicas no urbanas en despliegue de fibra propuestos por los Estados miembros. La banda ancha no es una inversión que pueda dejarse totalmente en manos del sector privado, y los incentivos de inversión, como permitir la facturación por uso, no asegurarán por sí mismos redes nacionales de fibra óptica hasta las instalaciones.

El despliegue de la red de fibra óptica hasta la central local no supone en sí mismo ninguna restricción importante sobre la capacidad actual: es el coste de la red de retorno de la central telefónica a Internet lo que supone una restricción (y en el futuro, el coste del cable de fibra óptica desde la central local al cliente). Todos los usuarios de banda ancha comparten la capacidad de la red de retorno desde la central local a Internet -capacidad que se debe comprar al por mayor al antiguo operador monopolista en la mayoría de los casos. Por lo tanto, estos operadores pueden controlar la capacidad disponible para los ISP competitivos. Burstein (2011) ha manifestado su convicción de que los límites actuales están diseñados para impedir la transmisión de vídeo *over-the-top* (OTT) por banda ancha, que compite con las ofertas de triple servicio de los ISP, que quieren que los abonados paguen por una línea telefónica, por servicio de banda ancha y por programación de vídeo servida por cable o Internet (también Crawford, 2011). El vídeo OTT podría competir con el último de estos servicios, y degradar o limitar el servicio de banda ancha puede proteger el servicio de vídeo del antiguo operador monopolista. Burstein estima los costes de la red de retorno para los ISP en menos de 1\$/mes, mientras que la Ofcom (2006) estimó que los costes de la red de retorno del servicio de repetición de vídeo del iPla-

yer de la BBC para los ISP del Reino Unido son del orden de 4-5 £/mes. Los precios han caído rápidamente con el aumento de la eficiencia de la transmisión en ese período (la Ley de Moore por sí sola habrá reducido los precios un 75% en cinco años). Se necesita mucha más investigación sobre los costes de la red de retorno y otras limitaciones de la facturación por uso.

2.1.2. Transparencia y gestión razonable del tráfico

Uno de los principios sobre neutralidad de la red promulgados tanto por la FCC como por la Comisión Europea es que solo se permitirá una «gestión de la red razonable», y que los usuarios finales deberán ser informados de dicho carácter razonable mediante información clara (Faulhaber, 2010). Tanto la FCC en Estados Unidos como la Comisión Europea han recurrido a declaraciones no vinculantes para dejar clara su intención de regular el carácter razonable de las prácticas de gestión del tráfico. En Canadá, la CRTC se ha basado en consultas, mientras que en Noruega y Japón por el momento no se ha exigido la observancia de las declaraciones no vinculantes de autorregulación.

La transparencia es una tarea en curso, y las mejores prácticas de regulación de la información todavía no han aparecido. Sin estas prácticas, cualquier compromiso con la neutralidad de la red es engañoso. Faulhaber (2010) ha sugerido cuatro principios básicos, a partir del examen de la regulación de la información en otras industrias: «1) revelar toda la información relevante para la elección del cliente, 2) a la que los clientes tengan acceso fácil, 3) con claridad y sencillez, y 4) de forma que sea verificable». Sostiene que Comcast no habría sido amonestada por la FCC si su gestión del tráfico hubiera sido más transparente. Sugiero un quinto principio: la información debe ser contrastada por una tercera parte, acreditada e independiente, que no dependa de la financiación de la industria de banda ancha, como una agencia de protección del consumidor. Esto podría llevarse a cabo de forma inde-

pendiente mediante un acuerdo autorregulación o de corrección.

Desde mayo de 2011, tanto las autoridades legislativas europeas como la Comisión Europea han tratado de definir la gestión razonable del tráfico a efectos de la legislación europea sobre el tráfico de Internet. Es probable que esto lleve a elaborar directrices más sólidas para los ISP y los consumidores (Sluijs, 2010), con un grupo de trabajo del ORECE que debe presentar un informe a finales de 2011. La normativa europea fue modificada en 2009 para incluir lo siguiente:

«19. Obligaciones de transparencia impuestas a los suministradores de redes de comunicaciones públicas que presten servicios de comunicaciones electrónicas disponibles para el público para garantizar la conectividad de extremo a extremo [...] la comunicación de todas las condiciones que limiten el acceso o la utilización de los servicios y aplicaciones cuando dichas condiciones sean autorizadas por los Estados miembros de conformidad con el Derecho comunitario y, cuando sea necesario y de forma proporcionada, el acceso por parte de las autoridades nacionales de reglamentación a la información necesaria para comprobar la exactitud de dicha comunicación.»¹

En el Reino Unido, Ofcom ha tratado de fomentar la autorregulación del sector con Códigos de Conducta sobre transparencia. También ha llevado a cabo una medición de las prácticas de los ISP en colaboración con SamKnows, una consultora que también ha trabajado con la FCC. SamKnows mide diecisiete indicadores en el periodo 2010-12.² Trabaja con Ofcom desde 2008 y con la FCC desde 2010 (con esta última está realizando 11 pruebas a lo largo de un período de tres años). Las pruebas de SamKnows con la FCC de Estados Unidos, en el proyecto llamado TestMyISP tienen también el apoyo de Measurement Lab, en particular, de la New America Foundation. La CRTC canadiense estableció reglas en 2009, pero hay pocas evidencias de que se haya exigido el cumplimiento de los principios de razonabilidad de la CRTC, que deben aplicarse caso por caso (Geist, 2011).

1. Anexo de la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas, según la modificación introducida por la Directiva 2009/140/CE de 25 de noviembre de 2009 (DOUE nº L 337, de 18 de diciembre de 2009).
2. Si desea obtener más información y consultar sus métodos, visite http://www.samknows.com/broadband/ofcom_and_samknows para Ofcom y <http://www.testmyisp.com/faq.html> para las pruebas de la FCC.

2.2. La transposición de las normas sobre neutralidad de la red

Las soluciones sobre neutralidad de la red establecidas en las Directivas europeas de 2009 tenían que haber quedado transpuestas en mayo de 2011. Dichas previsiones pueden clasificarse según el grado de autorregulación que implican, desde la comunicación informal básica hasta la reglamentación oficial. La tendencia general es ampliar el ámbito de la correulación, a menudo a expensas de la legislación. Existe una amplia variedad de modelos de herramientas de correulación (Unión Europea, 2003) para aquellas medidas que requieren una aplicación coordinada o conjunta (Marsden *et al.*, 2008; Tambini, Leonardí, Marsden, 2007). Sin una correulación que responda a la protección constitucional de la libertad de expresión a nivel nacional, las medidas no pueden autosostenerse (Marsden, 2011).

En el Reino Unido, Ofcom ha intentado continuamente desde 2008 alcanzar una solución de autorregulación. En 2011, con el calendario de transposición de las directivas de la Comisión Europea acercándose, el Broadband Stakeholder Group (BSG) financiado por el Gobierno elaboró un código de conducta, sobre el que el ministro del Gobierno del Reino Unido indicó que Berners Lee desempeñaría un papel de supervisión (Vaizey, 2011). A lo largo de 2012 se verá si semejante maltrecho acuerdo es capaz de satisfacer a la Comisión Europea, que tiene la obligación legal de inspeccionar la transposición. Es probable que primero pregunte a los 27 estados miembros los detalles de sus concretas transposiciones, antes de que se pueda solicitar más información, lo que sería el prelude de un posible caso ante el Tribunal de Justicia de la Unión Europea (TJUE). Es poco probable que un caso así se lleve ante el tribunal antes de 2013.

En Estados Unidos, la correulación es un concepto nuevo y la aplicación de los medios técnicos para medir la razonabilidad de la gestión del tráfico deberán probarse en un foro de autorregulación (aunque con la bendición de la FCC): el Grupo de Asesoría Técnica de la Industria de la Banda Ancha (Broadband Industry Technical Advisory Group [BITAG]), cuyo director ejecutivo es Dale Hadfield, un veterano de la FCC. Entre sus funciones específicas se halla la de ofrecer opiniones de salvaguarda (*safe harbors*) sobre las prácticas

de gestión del tráfico de las partes que solicitan formalmente un dictamen de asesoramiento técnico: «Las funciones específicas del grupo técnico de trabajo incluyen: i) identificar las “mejores prácticas” de los proveedores de banda ancha y otras entidades; ii) interpretar y aplicar prácticas de protección (*safe harbor practices*); iii) proporcionar orientación técnica al sector y al público; y/o iv) emitir opiniones de asesoramiento sobre los temas técnicos estrechamente relacionados con la misión del grupo técnico de trabajo que puedan subyacer en los conflictos entre distintas partes». (BITAG, 2011, sección 7.1). Los miembros del BITAG son un amplio número de grupos de interés y, por lo tanto, está lejos de ser simplemente una solución de autorregulación de la industria; pero cobra a las empresas por analizar sus soluciones, y de momento no está impuesto por la ley, de modo que sigue actuando como un foro de autorregulación y no de correulación.³

Como empresa legalmente constituida en Delaware, con estatutos publicados y una política de defensa de la competencia para excluir formalmente la intervención del Gobierno, la estructura del BITAG es la de una clásica entidad de autorregulación. Los académicos estadounidenses del campo del derecho y de las políticas podrían estar interesados en investigar cuáles son las ventajas y los costes en términos de control constitucional y de flexibilidad regulatoria, en comparación con las entidades europeas más basadas en el derecho administrativo. Phil Weiser ha propuesto apoyar un mecanismo de co-regulación (Weiser, 2009).

Como era de esperar, la regulación de la neutralidad de la red ha topado con la fuerte oposición de los ISP, y se ha llevado a cabo por vía de una serie de declaraciones y del establecimiento de condiciones para las fusiones, más que mediante una plena regulación a través reglamentos y leyes. Las fusiones dan a los reguladores la oportunidad de introducir estos relativamente pequeños ajustes, ya que las partes se hallan ansiosas por concluir el acuerdo global de fusión y están dispuestas a aceptar los inconvenientes relativamente poco importantes de controles sobre la gestión de tráfico a cambio de que se apruebe la fusión. De la misma manera que los consumidores -incluso con información perfecta- pueden no ver la cuestión de la gestión del tráfico como el elemento principal de su suscripción a la banda ancha (y por tanto, son presa fácil de condiciones restricti-

3. Para obtener más información, visite http://members.bitag.org/kwspub/BITAG_Membership/

vas, mientras los estándares de la industria impidan una capacidad real de elección entre ISP), también los ISP pueden tomar decisiones estratégicas de aceptar algunas condiciones restrictivas de gestión de tráfico como precio de aprobación de la fusión. La propuesta de fusión de AT&T Wireless y T-Mobile en 2011 también podría ilustrar la tendencia a imponer la neutralidad de la red mediante las condiciones de fusión, al igual que la fusión de Level3 y Global Crossing, importantes proveedores de red troncal de nivel 1 con vastas redes de distribución de contenidos.

2.3. ¿El caso especial de la neutralidad de la red en las redes inalámbricas o móviles?

El Internet móvil sigue siendo un pobre sustituto del Internet fijo. En 2010 los usuarios de *smartphones* (los usuarios de móviles más avanzados) solo descargaron una media de 79 megabytes por mes (Cisco, 2011). Resulta engañoso usar el crecimiento del porcentaje global para sugerir que hay un problema importante de congestión; al final, la gente usa Internet en redes móviles mediante *dongles* (módems USB) y *smartphones*, de modo que el uso absoluto se incrementa lentamente en comparación con el crecimiento. En 2010, el tráfico móvil fue de un total de 237 petabytes, lo que según Cisco es tres veces mayor que el tráfico total de Internet en el año 2000. Más relevante es que constituyó el 1% del tráfico de Internet en 2010, un total global de 21 exabytes. Si en la próxima década el tráfico móvil de datos crece el doble de rápido que el Internet global, ascenderá a un 11% de la totalidad del tráfico de Internet en 2020. En ese momento, se convertirá en algo más que una insignificancia estadística en términos globales. Las aseveraciones sobre el tráfico móvil se deben tomar con gran escepticismo ya que constituye una parte ínfima del total del tráfico medido de Internet, y de hecho se prevé que parte sustancial del tráfico móvil en el futuro será mediante femtoceldas, WIFI celular y otras infraestructuras de acceso inalámbrico fijo que se superpondrán al relativamente estable y maduro Internet fijo que se está ampliando para satisfacer la demanda de capacidad. El tráfico móvil es una proporción trivial del tráfico total de Internet por volumen, pero supone una prima importante por el servicio prestado en comparación con el tráfico fijo.

El grupo de reguladores europeos del ORECE (2010, pág. 11) declaró: «la red de acceso móvil puede necesitar poder limitar el consumo total de capacidad por usuario en determina-

das circunstancias (más que las redes de acceso fijas con elevados recursos de ancho de banda) y como esto no implica un tratamiento selectivo de contenido, no plantea, en principio, problemas de neutralidad de la red». El ORECE señala que, si bien las redes móviles siempre tendrán mayor necesidad de gestión de tráfico que las fijas («la gestión del tráfico para accesos móviles es más exigente»), se debe mantener una regulación simétrica para asegurar la neutralidad tecnológica: «no hay argumentos suficientes que justifiquen adoptar enfoques diversos en materia de neutralidad de la red en las redes fijas y en las móviles. Y en especial, una aproximación a la neutralidad de la red orientada al futuro no debe hacer distinciones entre distintos tipos de redes.» El ORECE (2010, pág. 3) llegó a la conclusión de que las redes móviles deben quedar sujetas a las previsiones de *net neutrality lite* de las Directivas 136/2009/CE y 140/2009/CE, señalando algunas infracciones de la neutralidad: «se han producido bloqueos de VoIP en redes móviles en Austria, Croacia, Alemania, Italia, los Países Bajos, Portugal, Rumania y Suiza». La encuesta Open Internet de la FCC solicitaba respuestas sobre la reglamentación de los servicios especializados gestionados y sobre la neutralidad en la red inalámbrica. La FCC anunció en su Orden (FCC, 2010) que estaba preparada para no imponer su regulación propuesta a los servicios inalámbricos en el futuro próximo. Esto implica que el mercado de Estados Unidos, más competitivo y con mayor crecimiento, estará menos regulado, mientras que el mercado europeo, más lento y menos competitivo, lo estará más.

3. El futuro: consideraciones de política pública en la neutralidad de la red

La neutralidad de la red es un tema políticamente más importante de lo que las autoridades de regulación de telecomunicaciones están preparadas o legalmente obligadas a examinar, ya que están en juego tecnologías de censura. El ORECE (2010, pág. 20) explica que:

«La libertad de expresión y los derechos ciudadanos así como el pluralismo de los medios de comunicación y la diversidad cultural son valores importantes de la sociedad moderna y son dignos de ser protegidos en este contexto, en especial porque la comunicación de masas se ha convertido en más fácil para todos los ciudadanos gracias a Internet. Sin embargo, la intervención en relación con tales consideraciones es algo que queda fuera de las competencias del ORECE».

«Poner una caja registradora en Internet» (Waclawsky, 2005) permitirá un conocimiento mucho más granular de lo que los clientes de un ISP descargan y cargan en Internet. Los ISP podrían filtrar tanto los contenidos molestos como los ilegales. Por ejemplo, podrían escuchar conversaciones delictivas, como las de los simpatizantes de terroristas, pornógrafos ilegales, acosadores, personas que planean robos, efectúan comentarios difamatorios, etc. También podrían ver las descargas ilegales de materiales con derechos de autor. En estas situaciones se verían obligados a cooperar con la policía o incluso con las industrias titulares de derechos de autor, lo que podría crear dificultades aún mayores cuando el contenido fuese legal en un país, pero ilegal en el país donde se reciba (Diebert *et al.*, 2010). Por tanto, la neutralidad de la red no es tan impopular entre los ISP pequeños que quieren evitar embrollos de responsabilidad legal; para evitar tales problemas se diseñaron específicamente la Directiva 2000/31/CE y otras normas nacionales de exención de responsabilidad de los ISP (safe harbors).

En 2011, los políticos estaban revisando la Directiva sobre comercio electrónico (Comisión Europea, 2010a, pág. 10-11) y aprobando leyes locales que favorecen, por ejemplo, a sus industrias de contenidos sujetos a derechos de autor, como la Ley de Economía Digital de 2010 en el Reino Unido o la ley HADOPI en Francia. En los debates para modificar el marco legal de las comunicaciones electrónicas a través de las Directivas 2009/136/CE y 2009/140/CE, los ISP europeos dominantes y con grandes recursos vieron la oportunidad de hacer causa común con los operadores móviles (Wu, 2007) y con otros, aliándose para impedir la transparencia y permitir el filtrado. La regulación de Internet está levantando barreras de entrada con la connivencia de los operadores principales, con consecuencias potencialmente muy graves para la libertad de expresión, la libre competencia y la expresión individual. Puede ser una opción correcta para una política de mayor seguridad en Internet (para evitar que los menores se vean expuestos a contenidos ilegales y/u ofensivos), si bien supone un abrupto cambio respecto del Internet abierto (Zittrain, 2008). Por tanto, es vital que los reguladores aborden la cuestión del correcto tratamiento de la neutralidad *lite*, para evitar daños al Internet actual, así como que empiecen a tratar la cuestión más compleja de las infracciones positivas –o por niveles– de la neutralidad de la red.

Las formas de censura privada realizada por intermediarios privados han ido en aumento a lo largo de la última década, aun cuando la ley sigue considerando a los intermediarios (principalmente ISP, pero también cada vez más empresas

de alojamiento de vídeos, como YouTube, redes sociales como Facebook y proveedores de servicios de búsqueda como Google) como los tres monos sabios que ni ven, ni oyen ni hablan. Estos intermediarios no son responsables del contenido de sus clientes según la Directiva sobre comercio electrónico (CE/2000/31) siempre y cuando no tengan conocimiento efectivo ni indiciario de dicho contenido, es decir, si «no oyen ningún mal, no ven ningún mal, y no hablan ningún mal» (Marsden, 2010a, pp. 105-149). Cualquier solución de neutralidad de la red tiene que ser integral, teniendo en cuenta el papel de los ISP en la ronda de negociaciones.

Las consultas sobre privacidad también pueden tener un impacto sobre el control regulatorio de la gestión del tráfico, con el Gobierno del Reino Unido llevado ante el Tribunal de Justicia por la Comisión Europea por aprobar las prácticas secretas e invasivas de publicidad basada en comportamiento de British Telecom y PHORM en 2006. La introducción de reglas de neutralidad de la red en la legislación europea se hizo bajo la rúbrica de las garantías de información al consumidor y de regulación de la privacidad, no de las leyes sobre competencia; y el Congreso de los Estados Unidos en 2011 estaba explorando activamente reglas de privacidad y controles sobre las actividades de publicidad comportamental de los ISP.

Finalmente, el reglamento aprobado en el otorgamiento de licencias puede afectar a la neutralidad de la red a un nivel fundamental. Los requisitos de interoperabilidad pueden servir de base para la acción cuando un ISP bloquea una aplicación. Además, se puede obligar a los ISP inalámbricos a dar acceso abierto, como en la subasta de la FCC de las frecuencias 700 MHz Upper Block C en 2008 (Rosston y Topper, 2010: 115-116) o en los requisitos generales de servicio público (*common carriage*) tradicionalmente impuestos a las redes públicas de comunicaciones desde antes de la aparición de las comunicaciones modernas, con los ferrocarriles y los telégrafos (Ley de ferrocarriles de 1844).

3.1. El desarrollo futuro de Internet y de la neutralidad de la red

El futuro de Internet no es un asunto trivial, de hecho es fundamental para el futuro de la productividad en la mayoría de las industrias. Es una tecnología posibilitadora, lo que significa que el intercambio de información en esta plataforma abierta promete (y consigue) eficiencias reales en la economía y en la sociedad en general, ya que facilita la colabora-

ción y la mejora (Carnoy *et al.*, 1993). También hace socialmente posible la Web 2.0 o web participativa (Schrage, 2000; Seely Brown y Duguid, 2000). Es decir, se ha convertido en patio de juego, clase, laboratorio y sala de chat virtuales (Palfrey y Gasser, 2008; Tapscott, 1999). Además, las pequeñas empresas y los trabajadores independientes que trabajan en casa dependen de Internet. La promesa de mundos virtuales y colaboración masiva *online* extenderá este impacto aún más en 2020.

En su análisis *Wealth of Networks*, Benkler (2006) piensa en Internet como un experimento gigante que combina el laboratorio con la innovación y comentarios de los usuarios, mientras que Boyle (2008) describe un movimiento más amplio en *Enclosing the Commons of the Mind* y Post (2009) realiza una comparación con la América jeffersoniana. El Internet abierto es un patrimonio común que todos deben poder disfrutar. Esta es la base de las reivindicaciones que exigen que ese patrimonio común se preserve, y que se promueva regulación que impida que ese bien común se cierre más y a la vez se asegure que los oportunistas o *free-riders* no lo arruinan, esto es, que no haya «tragedia de los comunes». El Internet abierto no es en modo alguno el único lugar para la formación de la opinión pública, ni necesariamente el más importante, pero es el espacio público abierto que confiere legitimidad a todos esos espacios privados o semi-privados.

Los problemas del desarrollo y la brecha digital global están estrechamente ligados con la neutralidad de la red. La conectividad a Internet es aún muy cara para la mayoría de los países en desarrollo, a pesar de los intentos de asegurar puntos locales de intercambio de Internet y nuevos cables submarinos, por ejemplo, para África oriental. Inundar los ISP del mundo en desarrollo con tráfico de vídeo, la mayoría del cual procede de los principales países de producción de vídeo, como India, Nigeria y, por supuesto, Hollywood, podría poner a los ISP locales en grave peligro financiero. Víctimas en estas empresas son, por ejemplo, países incluidos en una lista negra por los ISP más importantes por producir grandes cantidades de *spam*: los consumidores nigerianos descubrieron que su correo electrónico estaba bloqueado debido a que sus ISP también eran usados por *spammers*. El segundo problema de desarrollo sobre el que se centra el debate sobre la neutralidad de la red es el acceso inalámbrico a Internet. La mayoría de los ciudadanos de los países en desarrollo tienen un ancho de

banda mucho menor que en Occidente y la mayor parte de su conexiones son móviles: India es probablemente el mejor ejemplo, un país con al menos diez veces más usuarios de móviles que de teléfonos fijos. En los próximos años, los usuarios de Internet del mundo en desarrollo van a poner a prueba los límites de las redes móviles, y tanto la capacidad como el precio podrían determinar hasta qué punto pueden esperar un rápido desarrollo o bien una experiencia tercermundista de Internet. Llamo la atención sobre cuestiones de desarrollo porque resultan críticas. El servicio universal es todavía un sueño inalcanzable para muchos en el mundo en desarrollo, y cuando llegue, la definición que se le dé determinará el umbral mínimo que los ISP tendrán que alcanzar. Como señala Mueller (2007, pág. 7), la neutralidad de la red «debe abarcar también una afirmación positiva del valor social, económico y político del acceso universal y no discriminatorio a los recursos de Internet entre las personas conectadas a Internet».

Los tipos de no neutralidad de la red empleados en Asia occidental/África septentrional en el invierno de 2010-11 tenían motivos políticos más que económicos, es decir, era una censura política diseñada para impedir el acceso de los ciudadanos a Internet. Mueller (2007, pág. 8) sostiene que la tendencia de los gobiernos tanto de regímenes represivos como tradicionalmente democráticos de obligar a los ISP a censurar el contenido por diversos motivos es un argumento a favor de una fuerte política de no intervención. Esto es especialmente valioso en los países donde hay mucho menos debate sobre cómo el gobierno, al obligar a los ISP a censurar contenidos, puede poner en peligro la privacidad del usuario y la libertad de expresión. Mueller sugiere que la metáfora de la neutralidad de la red se podría usar para sacar a la luz todos los filtros y prácticas de censura, así como otras áreas de la regulación de Internet, como la gobernanza de los nombres de dominio. La neutralidad en la red se ha convertido en un importante problema debatido en el Foro de Gobernanza de Internet (FGI) de las Naciones Unidas. Los debates del FGI sobre neutralidad de la red han aumentado considerablemente (FGI, 2008, 2009).

Podemos esperar más actos de protesta de los internautas que no están de acuerdo con las políticas de neutralidad de la red, especialmente cuando consideren que los ISP no han informado correctamente a los usuarios finales sobre las implicaciones de los cambios de política. Se

cuestiona públicamente a los reguladores y a los políticos por este tipo de problemas, sobre todo dada la ubicuidad del correo electrónico, Twitter y las protestas contra la censura organizadas mediante las redes sociales, y se han elegido dos diputados del Partido Pirata en el Parlamento Europeo. La investigación sobre el activismo social contra el control empresarial de Internet es cada vez mayor (Hart, 2011).

4. Conclusiones: investigación de política futura

La evolución de Internet es dinámica y compleja. La disponibilidad y diseño de una respuesta de regulación adecuada debe reflejar ese dinamismo, y también la capacidad de los reguladores y los operadores de darse respuesta mutuamente. Así pues, la legislación nacional debe ser válida para el futuro y no ser excesivamente prescriptiva para evitar una respuesta prematura al entorno emergente. El ritmo al que cambia la relación entre arquitectura y contenido en Internet requiere una continua mejora en la investigación y la formación tecnológica del regulador. Los reguladores pueden monitorizar tanto las transacciones comerciales como la gestión del tráfico de los ISP para detectar posibles discriminaciones abusivas. Un requisito *ex ante* de mostrar las métricas internas de tráfico a los clientes proveedores de contenido, estableciendo un requisito de información por vía de regulación o de correulación, puede ser una solución práctica. La necesidad de mejor investigación para comprender la naturaleza de los problemas de con-

gestión en Internet y su efecto sobre el contenido y la innovación es clara (Marsden *et al.*, 2008). Estas conclusiones apoyan la idea de un régimen regulatorio mínimo que comprenda requisitos de información y correulación, junto con, en la medida de lo posible, soluciones de mercado. Las soluciones pueden ser tanto internacionales como locales, y la coordinación internacional de las mejores prácticas y conocimiento permitirá a los reguladores nacionales no quedarse atrás en la carrera tecnológica.

La base jurídica europea para la intervención regulatoria es un marco habilitador para prevenir los abusos y la discriminación, y en dicho marco los reguladores nacionales necesitan habilidades y pruebas para investigar la discriminación injustificada. Hay que advertir a los reguladores que no pueden limitarse a la postura reactiva de esperar a que se les presenten pruebas evidentes. Un enfoque más proactivo en la monitorización e investigación de prácticas no neutrales hará que los operadores de redes sean mucho más conscientes de sus deberes y obligaciones. Una intervención orientada a los consumidores y ciudadanos se basa en impedir que se ejerzan controles no regulados y opacos sobre el tráfico, ya sean impuestos por los ISP para obtener ventajas financieras o por gobiernos deseosos de aprovechar esta nueva tecnología para filtrar, censurar y hacer respetar derechos de autor contra sus ciudadanos. Deshacer el previo régimen de responsabilidad limitada de los ISP conlleva el riesgo de eliminar la eficiencia con que dicho sistema permite el libre flujo de información para beneficio de la economía y de la sociedad.

Referencias

- AMMORI, M. (2010). «How I lost the big one bigtime». <<http://ammori.org/2010/04/07/how-i-lost-the-big-one-bigtime>>
- AYRES, I.; BRAITHWAITE, J. (1992). *Responsive regulation. Transcending the deregulation debate*. Hartford, CT: Yale University Press.
- BAUER, Johannes M. (2010). «Learning from each other: promises and pitfalls of benchmarking in communications policy». *Info*. Vol. 12, n.º 6, pág. 8-20.
- BENKLER, Y. (1998a). «Communications infrastructure regulation and the distribution of control over content» [en línea]. *Telecommunications Policy*. Vol. 22, n.º 3, pág. 183-196. <<http://www.benkler.org/PolTech.pdf>>
- BENKLER, Y. (1998b) «Overcoming agoraphobia: building the commons of the digitally networked environment» [en línea]. *Harvard Journal of Law and Technology*. Vol. 11, n.º 2, pág. 287-400. <<http://jolt.law.harvard.edu/articles/pdf/v11/11HarvJLTech287.pdf>>

- BENKLER, Y. (2006). *The wealth of networks. How social production transforms markets and freedom*. New Haven, CT y Londres: Yale University Press.
- BERNERS LEE, Tim (2006). «Net neutrality: this is serious». [21/06/2006, 16:35]. <<http://dig.csail.mit.edu/breadcrumbs/node/144>>
- BITAG (2011). *By-laws of Broadband Industry Technical Advisory Group*. <http://members.bitag.org/kwspub/background_docs/BITAG_Bylaws.pdf>
- BOYLE, J. (2008). *The public domain: enclosing the commons of the mind*. New Haven, CT: Yale University Press.
- BURSTEIN, D. (2008). «Comcast's fair 250 gig bandwidth cap». *Fast Net News*. DSL Prime, Docsis report, 21 octubre. <<http://www.dslprime.com/docsisreport/163-c/53-comcasts-fair-250-gig-bandwidth-cap>>
- BURSTEIN, D. (2011). «Wireline costs and caps: a few facts». *Fast Net News*. DSL Prime, 6 marzo. <<http://www.dslprime.com/dslprime/42-d/4148-costs-and-caps>>
- CARNOY, M.; CASTELLS, M.; COHEN, S. S.; CARDOSO, F. H. (1993). *The new global economy in the information age; reflections on our changing world*. Nueva York: Macmillan.
- CAVE, M.; VAN EIJK, N.; PROSPERETTI, L. [et al.] (2009). «Statement by European academics on the inappropriateness of imposing increased Internet regulation in the EU». 8 enero 2009. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1329926>
- CHERRY, Barbara A. (2006). «Misusing network neutrality to eliminate common carriage threatens free speech and the postal system». *Northern Kentucky Law Review*. Vol. 33, n.º 4, pág. 483-511.
- CHERRY, Barbara A. (2008). «Back to the future: how transportation deregulatory policies foreshadow evolution of communications policies». *The Information Society*. Vol. 24, n.º 5, pág. 273-291.
- CISCO (2011). *Cisco visual networking index: global mobile data traffic forecast update, 2010-2015*. <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html>
- CLARK, David D. (1988). «The design philosophy of the DARPA Internet protocols». *Computer Communications Review*. Vol. 18, n.º 4, agosto, pág. 106-114.
- CLARK David D.; BLUMENTHAL, Marjory S. (2011). «The end-to-end argument and application design: the role of trust». *Federal Communications Law Journal*. Vol. 63, n.º 2, pág. 357-390.
- Código noruego (2009). «Guidelines for net neutrality». <<http://www.npt.no/iKnowBase/Content/109604/Guidelines%20for%20network%20neutrality.pdf>>
- Comcast v. FCC (2010). Sentencia del tribunal de apelaciones de los Estados Unidos, Circuito del Distrito de Columbia, del 6 de abril. N.º 08-1291. <<http://pacer.cadc.uscourts.gov/common/opinions/201004/08-1291-1238302.pdf>>
- COMISIÓN EUROPEA (2002). Better regulation action plan. COM 278. Bruselas.
- COMISIÓN EUROPEA (2010a). *A digital agenda for Europe*. COM 245. Bruselas. <http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf>
- COMISIÓN EUROPEA (2010b). *Consultation on the future of the universal service obligation*. <http://ec.europa.eu/information_society/policy/ecommlibrary/public_consult/univeuniv_service_2010/index_en.htm>

- CRAWFORD, S. (2011). *The big squeeze: the looming cable monopoly* [en preparación].
- CROWCROFT, J. (2011). «The affordance of asymmetry or a rendezvous with the random?». *Communications and Convergence Review*. Vol. 3, n.º 1.
- CRTC (2011). *Usage-based billing for Gateway Access Services and third-party Internet access services*. Telecom Decision 2011-44. File number: 8661-C12-201015975. Ottawa, 25 enero 2011. <<http://www.crtc.gc.ca/eng/archive/2011/2011-44.htm>>
- DE BEER, J. (2009). «Network neutrality in the Great White North (and its impact on Canadian culture)». *Telecommunications Journal of Australia*. Vol. 59, n.º 2, pág. 24.1-24.19.
- DE SOLA POOL, I. (1983). *Technologies of freedom*. Cambridge MA: Belknap.
- DEIBERT, R. J.; PALFREY, J. G.; ROHOZINSKI, R.; ZITTRAIN, J. (eds) (2010). *Access controlled: the shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.
- Digital Economy Act (2010). <<http://www.legislation.gov.uk/ukpga/2010/24/contents>>
- DONAHUE, H. (2010). «The network neutrality inquiry». *Info*. Vol. 12, n.º 2, pág. 3-8.
- DUNSTONE, C. (2006). *Presentation by Carphone Warehouse/TalkTalk CEO at the 2006 Ofcom conference*. <<http://www.ofcom.org.uk/event/2006conference/presentations/session3>>
- ECONOMIDES, N.; TÁG, J. (2007). *Net neutrality on the Internet: a two-sided market analysis*. Working Paper. Nueva York: NYU Center for Law and Economics.
- FAULHABER, Gerald R. (2002). «Network effects and merger analysis: instant messaging and the AOL-Time Warner case». *Telecommunications Policy*. Vol. 26, n.º 5-6, pág. 311-333.
- FAULHABER, Gerald R. (2010). «Transparency and broadband Internet service providers». *International Journal of Communication*. Vol. 4, pág. 738-757
- FCC (2005). *Appropriate framework for broadband access to the Internet over wireline facilities et al*. Policy statement, 20 FCC Rcd 14986 (2005). (Internet policy statement).
- FCC (2010). *In the matter of preserving the open Internet broadband industry practices*. GN Docket No. 09-191, WC Docket No. 07-52. Report and order. Adopted: 21 diciembre 2010.
- FGI (Foro de Gobernanza de Internet (FGI) (2008). «Network neutrality: examining the issues and implications for development». *Co-hosted workshop*, 4 diciembre. <<http://techpolicyinstitute.org/events/show/77.html>> y <<http://www.intgovforum.org/cms/index.php/2008-igf-hyderabad/event-reports/72-workshops/370-workshop-58-network-neutrality-examining-the-issues-and-implications-for-development>>
- FGI (Foro de Gobernanza de Internet (FGI) (2009). *Programme, format and schedule for the 2009 meeting*. Revisión del 4 de junio de 2009. <<http://www.intgovforum.org/cms/2009/postings/ProgrammePaper.04.06.2009.rtf>>
- FRIEDEN, Rob (2010a). *Winning the silicon sweepstakes: can the United States compete in global telecommunications?* Hartford, CT: Yale University Press.
- FRIEDEN, Rob (2010b). «Invoking and avoiding the First Amendment: how Internet service providers leverage their status as both content creators and neutral conduits». *The Journal of Constitutional Law*. Vol. 12, n.º 5, pág. 1279-1324. University of Pennsylvania Law School.
- FRIEDEN, Rob (2011). «A layered and nuanced assessment of network neutrality rationales». En: *Tilburg TILEC Workshop on Law and Economics*, 20 junio. <<http://www.tilburguniversity.edu/research/institutes-and-research-groups/tilec/pdfs/events/20-21june2011/paper-robert-frieden.pdf>>

- GAINES, S. E.; KIMBER, C. (2001). «Redirecting self-regulation». *Environmental Law*. Vol. 13, n.º 2, pág. 157-184.
- GEIST, Michael (2011a). «Unpacking the policy issues behind bandwidth caps & usage based billing». 1 febrero.
<<http://www.michaelgeist.ca/content/view/5611/99999/>>
- GEIST, Michael (2011b). «Canada's usage based billing controversy: how to address the wholesale and retail issues». Marzo 2011.
<http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,53/>
- HARRIS, Susan; GERICH, Elise (1996). «Retiring the NSFNET backbone service: chronicling the end of an era». *ConneXions*. Vol. 10, n.º 4, abril.
<www.merit.edu/networkresearch/projecthistory/nsfnet/nsfnet_article.php>
- HART, Jeffrey A. (2011). «The net neutrality debate in the United States». *Journal of Information Technology & Politics*. N.º 1, 2011, pág. 1.
- HASLINGER, Gerhard; NUNZI, Giorgio; MEIROSU, Catalin; FAN, Changpeng; ANDERSEN, Frank-Uwe (2011). «Traffic engineering supported by Inherent Network Management: analysis of resource efficiency and cost saving potential». *International Journal of Network Management*. Vol. 21, n.º 1, pág. 45-64, enero-febrero. DOI: 10.1002/nem.770.
- KIEDROWSKI, T. (2007). «Net neutrality: Ofcom's view».
<http://www.radioauthority.org.uk/media/speeches/2007/02/net_neutrality>
- LABOVITZ, C; IEKEL-JOHNSON, S.; MCPHERSON, D.; OBERHEIDE, J.; JAHANIAN, F.; KARIR, M. (2009). *ATLAS Internet Observatory Annual Report, and their presentation to the North American Network Operators Group - an industry body - NANOG (2009)*.
<http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf>
- LEMLEY, M. A.; LESSIG, L. (1999). *Ex Parte declaration of Professor Mark A. Lemley and Professor Lawrence Lessig in the matter of: application for consent to the transfer of control of licenses of Mediaone Group, Inc. to AT&T Corp, CS Docket No. 99-251, before the Federal Communications Commission*.
- LESSIG, L. (1999a). *Code and other laws of cyberspace*. Nueva York: Basic Books.
- LESSIG, L. (1999b). «The limits in open code: regulatory standards and the future of the Net». *Berkeley Technology Law Journal*. Vol. 14, n.º 2, pág. 759-770.
- LESSIG, L.; WU, T. (2003). *Letter to the FCC Ex parte*, 22 agosto 2003.
<www.timwu.org/wu_lessig_>
- MALIK, O. (2010). «U.S. mobile data traffic to top 1 exabyte». 7 noviembre.
<<http://gigaom.com/2010/11/07/in-2010-us-mobile-data-traffic-to-top-1-exabyte/>>
- MARSDEN, C. (2001). «The start of end-to-end? Internet protocol television». *Intermedia*. N.º 29, pág. 4-8.
- MARSDEN, C. (2010a). *Net neutrality: towards a co-regulatory solution*. Londres: Bloomsbury Academic.
- MARSDEN, C. (2010b). «Appeals Court demolishes FCC legal argument for ancillary jurisdiction without Title I argument in Comcast». 6 abril.
<<http://chrismarsden.blogspot.com/2010/04/appeals-court-demolishes-fcc-legal.html>>

- MARSDEN, C. (2011). *Internet co-regulation: European law and regulatory legitimacy in cyberspace*. Cambridge: Cambridge University Press.
 <http://www.cambridge.org/gb/knowledge/isbn/item6445008/?site_locale=en_GB>
- MARSDEN, C.; CAVE, J. *et al.* (2006). *Assessing indirect impacts of the EC proposals for video regulation, TR-414 for Ofcom*. Santa Monica, CA: RAND.
- MARSDEN, C.; SIMMONS, S.; BROWN, I.; WOODS, L.; PEAKE, A., ROBINSON, N. *et al.* (2008). «Options for and effectiveness of Internet self- and co-regulation phase 2: Case study report». 15 enero 2008. Prepared for European Commission DG Information Society & Media.
 <<http://ssrn.com/abstract=1281374>>
- MAYER-SCHONBERGER, V. (2008). «Demystifying Lessig». *Wisconsin Law Review*. N.º 4, pág. 713-746.
- MEISEL, J. P. (2010). «Trinko and mandated access to the Internet». *Info*. Vol. 12, n.º 2, pág. 9-27.
- MINTS (2007). *Methodology*. Página actualizada el 30 de agosto.
 <<http://www.dtc.umn.edu/mints/methodology.html>>
- MINTS (2009). *MINTS pages updated, many new reports, further slight slowdown in wireline traffic growth rate*. 17 noviembre.
 <http://www.dtc.umn.edu/mints/news/news_22.html>
- MUELLER, M. (1998). *Universal service: competition, interconnection, and monopoly in the making*. Washington DC: AEI Press.
- MUELLER, M. (2007). «Net neutrality as global principle for Internet governance». Internet Governance Project Paper IGPO7-003.
 <<http://internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf>>
- NOAM, E. M. (1994). «Beyond liberalization II: the impending doom of common carriage». *Telecommunications Policy*. Vol. 18, n.º 6, pág. 435-452.
- NOAM, E. M. (2008). «Beyond net neutrality: enduser sovereignty». Columbia University Draft Paper for 34th Telecoms Policy Research Conference, 14 agosto.
- OCDE (2008). *OECD Broadband portal, table 5(m): Time to reach bit/data caps at advertised speeds*. Septiembre 2008.
 <<http://www.oecd.org/dataoecd/11/15/39575302.xls>>
- OCDE (2010). *OECD Broadband portal, table 1l: Percentage of fibre connections in total broadband among countries reporting fibre subscribers*. Junio 2010.
 <<http://www.oecd.org/dataoecd/21/58/39574845.xls>>
- ODLYZKO, Andrew; LEVINSON, David (2007). «Too expensive to meter: the influence of transaction costs in transportation and communication» [borrador]. <<http://www.dtc.umn.edu/~odlyzko/doc/meteringexpensive.pdf>>
- OFCOM (2006). *Market impact assessment: BBC new on-demand video proposals*.
 <<http://stakeholders.ofcom.org.uk/market-data-research/tv-research/bbc-mias/ondemand/bbc-ondemand/>>
- OFTTEL (2000). *Draft Direction under Condition 45 of the Public Telecommunications Licence granted to British Telecommunications plc of a dispute between BT and MCI Worldcom concerning the provision of a Flat Rate Internet Access Call Origination product (FRIACO), noting at point 3 that «BT cited concerns about network capacity and the principle of capacity charging»*.
 <<http://www.ofcom.org.uk/static/archive/oftel/publications/internet/fria0400.htm>>

- ORECE (Organismo de Reguladores Europeos de las Comunicaciones Electrónicas) (2010). *BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe*. BoR (10) 42.
 <http://www.erg.eu.int/doc/berec/bor_10_42.pdf>
- PALFREY, J.; GASSER, U. (2008). *Born digital: understanding the first generation of digital natives*. Nueva York: Basic Books.
- POST, D. (2009). *In search of Jefferson's Moose: notes on the state of cyberspace*. Nueva York: Oxford University Press.
- REIDENBERG, J. (2005). «Technology and Internet jurisdiction». *University of Pennsylvania Law Review*. Vol. 153, n.º 6, p. 1951-1974.
- RENDA, A. (2008). *I own the pipes, you call the tune: the net neutrality debate and its (ir)relevance for Europe*. CEPS Special Reports. Bruselas: Centre for European Policy Studies.
- ROONEY, BEN (2011). «Net neutrality debate in Europe Is 'Over'». 28 febrero.
 <http://blogs.wsj.com/tech-europe/2011/02/28/net-neutrality-debate-in-europe-is-over/?mod=google_news_blog>
- ROSSTON, G. I.; TOPPER, M. D. (2010). «An anti-trust analysis of the case for wireless net neutrality». *Information Economics and Policy*. Vol. 22, n.º 10, pág. 103-119.
- SALTZER J. H.; REED, D.; CLARK, D. (1981). «End to end arguments in system design». En: *Second International Conf. on Distributed Computing Systems*, pág. 509-12.
- SCHRAGE, M. (2000). «The debriefing: John Seely Brown». *Wired*. N.º 8.08, agosto.
- SEELY BROWN J.; DUGUID, P. (2000). *The social life of information*. Cambridge, MA: Harvard Business School Press.
- SLUIJS, Jasper P. (2010). «Network neutrality between false positives and false negatives: introducing a European approach to American broadband markets». *Federal Communications Law Journal*. Vol. 62, pág. 77.
- TAMBINI, L.; MARSDEN, C. (2008). *Codifying cyberspace: communications self-regulation in the age of internet convergence*. Londres: Routledge.
- TAPSCOTT, D. (1999). *Growing up digital: the rise of the net generation*. Nueva York: McGraw Hill.
- TEUBNER, G. (1986). «The transformation of law in the welfare state». En: G. TEUBNER (ed.). *Dilemmas of law in the welfare state*. Berlin: W. de Gruyter.
- THINKBROADBAND (2009). *Average mobile broadband speed clocks in at 0.9 meg*. 10 junio.
 <<http://www.thinkbroadband.com/news/p/2.html>>
- UNIÓ EUROPEA (2003). *Inter institutional agreement*.
 <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF>>
- VAIZEY, Ed (2011). *Hansard HC Deb*, 5 abril 2011, c259WH.
 <<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110405/halltext/110405h0002.htm#11040557000591>>
- WACLAWSKY, J. G. (2005). «IMS 101: What you need to know now». *Business Communications Review*. Junio 2005, pág. 18-23.
 <http://109.69.9.58/wp-content/uploads/2011/10/03_waclawsky-18_Jun05.pdf>
- WEISER, P. (2009). «The future of Internet regulation». *U.C. Davis Law Review*. Vol. 43, n.º 2, pág. 529-590.

- WERBACH, Kevin (2005). «The Federal Computer Commission». *North Carolina Law Review*. Vol. 84, n.º 1, pág. 21.
- WERBACH, Kevin (2010). «Off the hook». *Cornell Law Review*. Vol. 95, pág. 535.
- WU, T. (2003a). «When code isn't law» [en línea]. *Virginia Law Review*. Vol. 89, pág. 679.
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=413201>
- WU, T. (2003b). «Network neutrality, broadband discrimination». *Journal of Telecommunications and High Technology Law* [en línea]. Vol. 2, pág. 141-172.
<<http://ssrn.com/abstract=388863>>
- WU, T. (2007). *Wireless net neutrality: cellular carterfone and consumer choice in mobile broadband*. New America Foundation Wireless Future Program Working Paper #17, febrero.
- YOO, C. (2010). «The changing patterns of Internet USAGE». *Federal Communications Law Journal*. Vol. 63, n.º1, pág. 67-90.
<http://www.law.indiana.edu/fclj/pubs/v63/no1/2010-Dec.-Vol.63-05_Yoo.pdf>
- ZITTRAIN, J. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale University Press.

Cita recomendada

MARSDEN, Christopher T. (2012). «Neutralidad de la Red: Historia, legislación y futuro». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 13, pág. 24-43. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-marsden_esp/n13-marsden_esp>

ISSN 1699-8154



Los textos publicados en esta revista están -si no se indica lo contrario- bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Acerca del autor

Christopher T. Marsden

<http://chrismarsden.blogspot.com/>

El doctor Christopher T. Marsden es profesor titular de Derecho de la Universidad de Essex desde 2007. Obtuvo una licenciatura en Derecho en 1989 y un máster en Derecho en 1994 en la London School of Economics y un doctorado en la Universidad de Essex. Es autor de *Net Neutrality: Towards a Co-regulatory Solution* (Bloomsbury, 2010), *Internet Co-regulation* (Cambridge University Press, 2011) y de 3 libros más como coautor o editor. Investiga sobre reglamentación sociolegal, reglamentación y la política de Internet y ha aparecido en artículos revisados por pares, informes de la Comisión Europea, gobiernos europeos, la OSCE y el Consejo de Europa, y autoridades legislativas nacionales y fundaciones. Fue analista senior de RAND Europa (2005-07), profesor en Warwick (1997-2000) y director de reglamentación/asesor general de proveedores de servicios de Internet y empresas de nueva creación (2000-3). Fue becario de investigación en Harvard's Kennedy School (1999), becario de Política Industrial en el Laboratorio de Computación de la Universidad de Cambridge (2006-8), profesor invitado en escuelas de Derecho en el Reino Unido, Estados Unidos, Japón, Australia.

University of Essex, School of Law
Wivenhoe Park
Colchester
CO4 3SQ Reino Unido

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la Red y otros retos para el futuro de Internet»

ARTÍCULO

El concepto de *net neutrality* y la tensión entre regulación pública y autorregulación privada de las redes*

Joan Barata Mir

Fecha de presentación: noviembre de 2011

Fecha de aceptación: noviembre de 2011

Fecha de publicación: febrero de 2012

Resumen

El término *net neutrality* (NN) se ha convertido hoy en día en un lugar común y en uno de los ejes de cualquier debate acerca de la regulación de la Red y de los contenidos, servicios y aplicaciones que circulan por ella. La idea de NN incide, esencialmente, en los términos en los que los ISP intervienen en los intercambios y comunicaciones que se producen entre, por un lado, usuarios finales, y por el otro, aquellos operadores que utilizan la plataforma de Internet para suministrar todo tipo de servicios y contenidos. El debate sobre la NN no es solo un debate económico que se mueva exclusivamente en el terreno de la defensa de la libre competencia en el mercado, tal y como se ha advertido anteriormente, la NN puede presentar también una clara vertiente de control de contenidos y por ello de incidencia en el ejercicio del derecho fundamental a la libertad de expresión y de información.

Palabras clave

Internet, regulación, redes, neutralidad

Tema

Ley sobre tecnologías informáticas

* Este artículo recoge los trazos fundamentales de la ponencia presentada el día 11 de julio del 2011 en el congreso «Internet, Derecho y Política. Neutralidad de la Red y otros retos para el futuro de Internet», organizado por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya. Elaborado en el marco del proyecto de investigación *Communications, Regulation and the Public Interest*, de la Facultad de Ciencias de la Comunicación Blanquerna (URL).

The Concept of Net Neutrality and the Tension between Public Regulation and Private Self-regulation of Networks

Abstract

The term net neutrality (NN) has today become commonplace and a central point in any debate on regulation of the Internet and the content, services and applications it offers. The idea of NN has a bearing, essentially, on those terms in which the ISPs intervene in exchange and communication between, on one hand the end user, and on the other, those operators who use the Internet as a platform to supply all kinds of services and content. The debate on NN is not only an economic one, restricted to the defence of free market competition. As commented previously, NN also takes on the significant aspect of control of content, and so affects the exercise of the fundamental right to freedom of expression and of information.

Keywords

Internet, regulation, networks, neutrality

Topic

IT Law

1. Introducción

El término *net neutrality* (NN) se ha convertido hoy en día en un lugar común y en uno de los ejes de cualquier debate acerca de la regulación de la Red y de los contenidos, servicios y aplicaciones que circulan por ella. Parecería, en principio, que cada vez que nos referimos a la NN estemos acudiendo a un concepto, acerca de cuyo significado existe un consenso entre juristas, economistas y especialistas en tecnología. Sin embargo, lo cierto es que ello no es necesariamente así. Es altamente probable que en cualquier discusión nominalmente dedicada a esta materia la noción de partida para cada uno de los intervinientes pueda ser distinta, condicionando ello, como es obvio, el análisis llevado a cabo. En consecuencia, la primera cuestión que se encuentra abierta en los debates acerca de la NN es la relativa a su propio significado.

Si hacemos un esfuerzo por elevar la vista y encontrar una noción mínima y común de NN, susceptible de ser aceptada por parte de cualquier participante en este debate, podremos convenir, de entrada, que se trata de un concepto vinculado a la garantía de un cierto nivel de apertura en el funcionamiento de la Red de Internet. En realidad, y esta es una primera consideración conceptual importante, tendremos que admitir que la idea de neutralidad no se aplicaría propiamente a las redes entendidas como infraestructuras físicas, sino a Internet como

concreta plataforma que permite el acceso a servicios, contenidos y aplicaciones. El concepto de NN incide pues en los términos y las condiciones a través de los cuales determinados actores o intermediarios de Internet tienen la capacidad de alcanzar a su destinatario final, situado en una de las terminaciones de dicha red. Y no se trataría de cualesquiera términos o condiciones, sino de aquellos sobre los cuales los proveedores de acceso a Internet (ISP) tienen a su vez la capacidad tecnológica de influir. En definitiva, la idea de NN alude al modo en el que los ISP pueden (o no) condicionar el acceso o comunicación recíproca a través de Internet entre usuarios finales y suministradores de contenidos, servicios y aplicaciones.

Vale la pena advertir que es difícil encontrar una red o plataforma de distribución que sea estrictamente neutral. Es evidente que sobre cualquier sistema de estas características inciden elementos estructurales, tecnológicos o incluso económicos que marcan una especie, si se quiere, de «pecado original», otorgando pues de entrada mayor capacidad de intervención a unos operadores que a otros. Piénsese, por ejemplo, en los debates acerca de los derechos de acceso, interconexión y desagregación de bucle local propios de los servicios de voz fija, o en el caso extremo de las redes ferroviarias. Si todo ello es así, una visión estrictamente neutral del funcionamiento de Internet como plataforma de comunicación en los términos antes reseñados supondría que los usuarios finales

deberían estar en condiciones de acceder a absolutamente cualquier proveedor, a velocidades y con niveles de calidad exactamente idénticos. Asimismo, una gestión de la Red estrictamente neutral por parte de los ISP obligaría a tratar del mismo modo a cualquier paquete, con independencia de que se trate de servicios con alto valor añadido o de un mero virus o *spam*. Si asumiéramos este punto de partida, entenderíamos como no neutral, y por ello contrario a la idea de NN, cualquier acción de los ISP orientada a bloquear virus, *spam* o a impedir la congestión de la Red, así como, por ejemplo, la oferta por parte de aquéllos servicios de Internet basados en la obtención, por parte del usuario final, de una mayor velocidad o capacidad de su conexión a Internet como contraprestación del pago de una tarifa más elevada.

Esta visión estrictamente igualitaria de la NN, que fue formulada en sus inicios por parte de uno de los primeros autores que han tratado la materia, Tim Wu, ha sido ya bastante apartada del actual debate, si bien que con relación a la misma se abren cuestiones controvertidas no resueltas, como es precisamente la de los niveles de calidad de conexión ofrecidos al usuario final.¹

En cualquier caso, y tratando de acotar unos mínimos elementos definitorios, vemos cómo la idea de NN incide, esencialmente, en los términos en los que los ISP intervienen en los intercambios y comunicaciones que se producen entre, por un lado, usuarios finales, y por el otro, aquellos operadores que utilizan la plataforma de Internet para suministrar todo tipo de servicios y contenidos. Si esto es así, una postura favorable a la NN supondría entender necesaria la garantía de que la intervención de los ISP en el señalado tráfico no obstaculizará indebidamente dichos intercambios (ya sea dando prioridad a unos proveedores frente a otros, ya sea bloqueando o haciendo muy difícil el acceso a determinadas ofertas). Ahora bien, ¿cuándo nos encontramos ante una obstaculización indebida, en definitiva, ante un abuso de la posición «natural» de dominio que cualquier ISP tiene sobre todo aquello que circula por la Red? Si prestamos atención al debate actual, veremos cómo dicho abuso podría hipotéticamente producirse a través de posibles acuerdos de los ISP con proveedores de contenidos o aplicaciones a fin de priorizar a éstos en su acceso por parte de

usuarios finales, o simplemente de decisiones directamente adoptadas por parte de los ISP, de priorizar aquellos servicios respecto de los cuales tienen un determinado interés económico (piénsese, por ejemplo, en los casos de concentración vertical). Este es, ciertamente, el núcleo duro del debate acerca de la NN.

Por otra parte, es obvio que habría otras formas de gestión no neutral de los paquetes que circulan por la Red que plantearía igualmente problemas desde el punto de vista de la protección de un determinado nivel de NN: pensemos en el supuesto en el que por parte de los ISP se lleve a cabo una inspección y restricción de determinados contenidos sobre la base de criterios netamente *editoriales*, es decir, primando contenidos de una determinada tendencia ideológica frente a otros, bloqueando contenidos originados en determinados países, etc.

2. La NN como parte de la tensión entre autorregulación y regulación propiamente dicha

La gestión de Internet, es decir, las condiciones y la velocidad de acceso a los contenidos, servicios y aplicaciones, así como las características técnicas de la conexión a Internet que permiten la óptima utilización de aquellos, se encuentra en buena medida en manos de los ISP. Este es un punto de partida fundamental para entender correctamente el resto de elementos del debate acerca de la aproximación regulatoria a la NN. Dicho de otro modo, los poderes públicos no tienen la capacidad técnica de control y de fiscalización directa de lo que sucede en la Red de Internet, al menos en lo que se refiere a las cuestiones que acaban de ser reseñadas.

Desde un punto de vista económico y tecnológico, la Red podría ciertamente autorregularse sobre la base de los acuerdos y, en definitiva, el juego de pesos y contrapesos que articula la compleja cadena de valor que existe en Internet como plataforma de distribución. A través de la Red circula un elevado valor económico mediante un gran número de intermediarios. Y lo cierto es que existe la posibilidad clara de que cualquiera de dichos intermediarios,

1. Véase Tim Wu (2003).

incluidos los ISP, pretendan sacar provecho de su posición e imponer determinadas condiciones o incluso ofrecer un trato especial a cambio de una contraprestación o de privilegiar sus concretos intereses económicos. Si aceptamos este sistema de autocomposición de intereses, habrá que asumir también el riesgo cierto de que el usuario final no pueda acceder a los servicios, aplicaciones y contenidos de su elección en estricta igualdad de condiciones y sobre la base de una auténtica libertad de decisión, sino que ello se encontrará estrictamente en manos de los distintos intervinientes de la cadena de valor, y de forma particular, aunque no exclusiva, de los ISP. Y digo de forma no exclusiva puesto que es evidente que otros actores como los grandes portales o motores de búsqueda tienen una evidente capacidad para incidir en los términos en los que un determinado usuario final acaba accediendo a un determinado contenido o aplicación.

Ciertamente, puede argumentarse que cualquiera de los operadores presentes en la Red presumiblemente tendría el incentivo económico de ofrecer a los usuarios finales la más amplia gama de contenidos y servicios sin limitación alguna, y de que en última instancia existirá siempre la garantía de la libre competencia, la cual debe permitir a aquellos cambiar de proveedor. Sin embargo, y sin perjuicio de las dificultades que este último elemento plantea y sobre las que no se puede entrar aquí, no hay ninguna evidencia a fecha de hoy de que dicho incentivo realmente exista, o al menos concurra en todos los casos. La presencia de competidores directos, la necesidad de evitar congestiones en las que determinados intereses salgan perjudicados, o bien la posición de «debilidad» en la que se pueden encontrar ciertos nuevos entrantes, son factores que pueden jugar, y de hecho juegan, un papel clave en supuestos actuales de gestión no neutral de las redes. Piénsese en este sentido en el caso de Comcast en los Estados Unidos, en los que dicha compañía de cable técnicamente bloqueó la descarga de contenidos audiovisuales a través de Bit Torrent, teniendo en cuenta que la compañía tenía su propia oferta de contenidos de pago, o en las dificultades que en la actualidad tiene cualquier usuario de una red de banda ancha de telefonía móvil para utilizar esta para realizar llamadas gratuitas a través de una plataforma tipo Skype.

Por consiguiente, si aceptamos como hipótesis factible (lo cual parece razonable) el hecho de que los ISP no tendrán siempre ni necesariamente el incentivo de gestionar neutralmente sus redes, puede entenderse como necesaria una intervención regulatoria propiamente dicha para garantizar dicha neutralidad. Es más, en términos de incentivos económicos, resulta plausible el hecho de que quienes deban realizar una fuerte inversión en redes que permitan posteriormente prestar servicios de acceso a Internet, aspiren a ostentar un cierto poder en lo que a la gestión de éstas se refiere, a obtener el máximo rendimiento económico de las capacidades técnicas que les proporcionan, así como, en última instancia, a obtener su «pedazo de pastel» con relación al valor económico que circula a través de dichas redes con la intervención decisiva, precisamente, de aquellos.

A partir de aquí, varios matices son necesarios. En primer lugar, hay que insistir en que no solo los ISP tienen la capacidad para alterar la gestión de la Red de acuerdo con una serie de parámetros de neutralidad. Según se ha advertido ya, grandes portales y motores de búsqueda conforman en cierta medida una especie de *hub* imprescindible en la dirección y redirección del tráfico de la Red, sobre la base de criterios y algoritmos que no resultan ni comprensibles ni transparentes para el usuario final. Si esto es así, es obvio que el papel de intermediación que a estos corresponde no es nada irrelevante en términos de «regulación del tráfico» y por ello constituyen un eslabón imprescindible en la garantía de la plena libertad de movimientos y de elección por parte de los usuarios de la Red. Sin embargo, el debate acerca de la garantía de ciertos principios en el ámbito de los señalados operadores se encuentra todavía bastante eclipsado por el de la NN propiamente dicha.²

En segundo lugar, hay que advertir también que la materia últimamente señalada se encuentra limitada a un ámbito muy concreto, cual es el del acceso por parte del usuario final a una oferta diversa de contenidos y aplicaciones, sin que exista un grado inaceptable de discriminación o simplemente de bloqueo con relación a determinadas partes de la misma. La pregunta que debemos plantearnos es si el poder de los ISP en materia de acceso es el único ámbito que resulta problemático en términos de gestión no neutral de la Red. Pensemos, por

2. Sobre estas cuestiones, véase Frank Pasquale (2008).

tomar solo un ejemplo, en la posibilidad de que, por parte de los ISP, pueda «venderse» a terceros información relevante acerca del funcionamiento de la Red y del comportamiento de los usuarios, que permita optimizar el uso de una determinada aplicación frente a otras. Por consiguiente, un análisis y estudio completo y pormenorizado acerca de posibles comportamientos no neutrales y no aceptables por parte de los ISP requiere seguramente de una comprensión mucho más amplia del funcionamiento de la Red y del papel y de las capacidades de estos, por lo que urge tomar conciencia de las limitaciones del enfoque actual.

En tercer lugar, hay que insistir en que el debate sobre la NN no es solo un debate económico que se mueva exclusivamente en el terreno de la defensa de la libre competencia en el mercado. Tal y como se ha advertido anteriormente, la NN puede presentar también una clara vertiente de control de contenidos y por ello de incidencia en el ejercicio del derecho fundamental a la libertad de expresión y de información. Dicho de otro modo, determinadas modalidades de comportamiento no neutral de los ISP (y no solo de dichos operadores) pueden consistir en la apertura de los paquetes transportados con la finalidad de seleccionar los contenidos que finalmente llegan al consumidor final, sobre la base de criterios de orientación política, sujeción a determinados límites en materia sexual, tipo de lenguaje empleado o incluso origen geográfico y lingüístico de aquellos. Es evidente que en tales supuestos nos encontraríamos claramente ante la censura privada de contenidos. Si aceptásemos esa práctica, la totalidad de los flujos expresivos que circulan por la Red dejarían de sujetarse, en su caso, a normas jurídicas propiamente dichas, para trasladar a manos de los gestores de la Red la función de regulación de la libre expresión y la libre circulación de la información. Un escenario, como puede suponerse, absolutamente indeseable en términos democráticos.

Finalmente, hay que señalar que la respuesta regulatoria a las carencias de neutralidad de las redes (en los términos en los que dicha noción ha sido aquí descrita), esto es, la regulación pública y externa frente a los efectos indeseados de una mera autorregulación operada entre los distintos eslabones de la cadena de valor, no ha sido hasta la fecha detalladamente caracterizada de modo consensuado. Es decir, el hecho de que se pueda llegar a un acuerdo acerca de la necesidad de garantizar un cierto nivel de apertura y neutralidad en el modo a través del

cual Internet permite el suministro y acceso a contenidos, servicios y aplicaciones, no cerraría de por sí el debate, puesto que a continuación sería necesario identificar con claridad cuáles serían los instrumentos regulatorios más idóneos a tal efecto.

Sin poder tampoco entrar aquí a fondo en tan importante y extensa materia, hay que señalar, en primer lugar, que una de las primeras cuestiones a plantear es hasta qué punto las normas vigentes en materia de derecho de la competencia (sobre todo en relación con las limitaciones a los abusos de posición dominante en el mercado) así como en materia de protección de los derechos fundamentales a la libertad de expresión y de información son suficientes para legitimar una prohibición de determinados comportamientos en el seno de Internet, de acuerdo con lo señalado hasta este momento. Otra cuestión fundamental a discernir, esencialmente por parte de los juristas, tiene que ver con la propia naturaleza jurídica de la neutralidad de la Red: ¿Es un derecho de cualquier ciudadano, susceptible de ser ejercido frente a terceros de acuerdo con los sistemas propios de garantía de cualquier derecho?, ¿es por el contrario un principio de la regulación de las redes, el cual tiene que ser respetado por parte del legislador y de la Administración en ejercicio de sus potestades?, ¿sería un mero criterio rector u objetivo no estrictamente vinculante, el cual se encontraría en última instancia vinculado a los criterios políticos que en cada momento y con relación a diversos tipos de redes y servicios puedan articularse, atendiendo asimismo a parámetros tales como los incentivos y el concreto nivel de inversión existente?

3. Medidas regulatorias vinculadas con la protección de la NN

La primera cuestión que vale la pena tratar con mayor detenimiento tiene que ver con algo que ha sido apuntado al principio de este texto: la vinculación del debate de la NN con la calidad del servicio prestado, especialmente en lo que se refiere a una posible discriminación de los precios pagados por el usuario final en función del ancho de banda utilizado y de la rapidez del acceso. Parece claro que, en la medida en que nos encontramos ante una materia no directamente vinculada con los suministradores de contenidos y aplicaciones, sino con los acuerdos a los que directamente puedan llegar los ISP con los consumidores

finales, la cuestión no entraría dentro del núcleo duro de los actuales debates acerca de la NN. Sin embargo, ello no quiere decir que no guarde relación alguna con la cuestión, en la medida en que los niveles de calidad condicionan, en última instancia, las posibilidades de disfrute de los servicios prestados por los distintos suministradores que operan en Internet. Así pues, una disminución de la calidad de la prestación del servicio de acceso puede acabar dando lugar a una situación en la que los consumidores finales no pueden disfrutar de determinadas aplicaciones o servicios. En estos casos, parecería insuficiente una justificación basada en el hecho de que «quien más paga, mejor servicio recibe» porque en realidad lo que sucedería sería una limitación efectiva de las condiciones de acceso, y en última instancia, de la apertura de la Red de Internet como plataforma de distribución. Ello explica, por ejemplo, que dentro de las extremadamente tímidas acciones de la Unión Europea en la materia, exista sin embargo una específica previsión en el artículo 22.3 de la Directiva sobre Servicio Universal de Comunicaciones Electrónicas (Directiva 2009/136/CE, de 25 de noviembre), en la cual se otorga a los reguladores nacionales la posibilidad de imponer determinados niveles de calidad del servicio en aquellos casos en los que exista el riesgo de una degradación significativa del mismo, con las consecuencias antes referidas.

En segundo lugar, un elemento regulatorio fundamental en materia de NN es el relativo a la transparencia. Este elemento presentaría una clara doble vertiente: por un lado, parece necesario que los usuarios finales conozcan, al menos, los criterios de gestión del tráfico que los ISP aplican con relación a su propia red. Por otra parte, y seguramente más importante, la transparencia debería vincularse, asimismo, con el suministro de información por parte de los ISP hacia el resto de operadores, de tal modo que puedan desarrollar los contenidos, aplicaciones y servicios que mejor se adapten a las características y tráfico de las redes en cada momento, optimizando así su uso y evitando en la medida de lo posible situaciones de colapso o estrangulamiento de las mismas. Tomada aisladamente, la transparencia quizá parecería una medida

muy simple, e incluso muchos la darían por supuesta. Sin embargo, y tal como se ha señalado, lo que realmente sucede dentro del tráfico de una determinada red no se encuentra expuesto al público ni a los reguladores, por lo que la imposición, correctamente detallada y articulada para su efectiva aplicación y cumplimiento, del deber de hacer público y accesible las capacidades y los modos de gestión del tráfico en las redes, se nos aparece como una medida realmente importante en materia de NN (en cualquiera de sus sentidos) y un punto de partida imprescindible para la discusión de medidas regulatorias más intensas o específicas.

Esta es, de hecho, la primera de las directrices regulatorias incluida en la Open Internet Order recientemente aprobada por parte de la Federal Communications Commission (FCC) y publicada oficialmente el 21 de septiembre previamente a su entrada en vigor el 20 de noviembre del 2011. Hay que advertir que el debate acerca de la necesidad de aprobación de una normativa que garantice un determinado nivel de NN en la banda ancha estadounidense ha formado parte de las discusiones políticas de los últimos años, y de hecho, la FCC había dado ya algunos pasos en ese terreno³ y adoptado incluso una notoria resolución en el conocido como caso ComCast, anteriormente mencionado.⁴ Pues bien, la regulación finalmente elaborada por parte de la FCC parte del establecimiento de una obligación general de transparencia, no necesariamente precisa en cuanto a su alcance específico, pero saludada por el conjunto de actores presentes en el debate como positiva.

En tercer lugar, parece obvio que el bloqueo injustificado de servicios, contenidos y aplicaciones, impidiendo pues el acceso a una parte de la oferta presente en Internet, resultaría inaceptable de acuerdo con parámetros, hay que insistir en ello, que no solo se refieren a la defensa de la libre competencia en el mercado, sino a la propia idea de la protección de la libre expresión en Internet. Cuestión distinta es el alcance del término *injustificados* que acabamos de utilizar, lo cual nos abre la puerta a las cuestiones vinculadas a la gestión del tráfico en la Red. En

3. Una explicación mínimamente pormenorizada de esa evolución se puede encontrar en el artículo Juan Carlos Laguna de Paz (2009). Téngase en cuenta también que previamente la autoridad canadiense de regulación de las comunicaciones había adoptado también una interesante decisión en relación con la materia. Ver Canadian Radio-Television and Telecommunications Commission (2009).

4. Ver Federal Communications Commission (2008).

esta misma línea, la decisión de la FCC mencionada prohíbe tanto el bloqueo injustificado de contenidos y aplicaciones como su discriminación no razonable.

En este terreno cobra especial relevancia la idea de gestión razonable de las redes a fin de evitar la congestión de las mismas o la circulación de contenidos que son claramente «nocivos», entendiéndolo en todo caso dicha noción de nocividad en términos exclusivamente técnicos. Es claro, en este sentido, que la detección y eliminación o no priorización de *spam*, virus y otras formas de basura cibernética entrarían dentro de las capacidades atribuibles a un ISP, e incluso podrían serle exigibles en términos de obligación de mantenimiento de las distintas rutas por las que viajarán los contenidos «legítimos» de la Red. No es tan claro, sin embargo, el modo a través del cual, en su caso, debería redactarse y articularse la correspondiente regulación en ese terreno: ¿cuál sería el margen de libertad de decisión de los ISP? ¿Sería exigible una proporcionalidad estricta en el sentido de aplicar la medida tecnológica que sea menos discriminatoria independientemente de su coste? ¿Cómo se vincula dicho «principio» con un hipotético deber de inversión en la construcción y mantenimiento de redes eficientes? Las respuestas a las anteriores preguntas pueden condicionar en gran medida la efectividad de las medidas a adoptar e incluso incidir en los incentivos de inversión de los titulares de las redes. En el caso de la decisión de la FCC, los términos excesivamente genéricos, ambiguos y poco restrictivos en los que se habilita a los ISP para tomar decisiones en ese terreno han dado lugar a un buen número de críticas por parte de una parte de los distintos operadores.

Otra cuestión de interés que debemos plantear es hasta qué punto una hipotética regulación de la NN debe ser a su vez tecnológicamente neutral. Es decir ¿debemos aplicar y exigir los mismos criterios de neutralidad a cualesquiera redes, sean fijas o móviles, independientemente de

los niveles de competencia y eficiencia alcanzados e independientemente de los incentivos a la inversión existentes? Más concretamente, ¿sería sostenible en la actualidad imponer a las redes móviles actualmente en desarrollo y despliegue obligaciones estrictas en materia de neutralidad (tal y como, por otra parte, sucede en los Países Bajos,⁵ mientras en Estados Unidos la FCC se niega rotundamente a ello)? Por otra parte, ¿debemos tratar por igual redes de uso doméstico y comercial y redes que permiten el acceso a Internet en puntos críticos e intensivos, en términos de interés general como espacios públicos, aeropuertos, determinadas infraestructuras, etc.? Esta es una cuestión especialmente delicada y relevante, vinculada directamente con el futuro desarrollo de redes de nueva generación en nuestros entornos inmediatos y que en buena medida queda pendiente de resolver.

Finalmente, una última cuestión de interés radica en la posibilidad de que las capacidades aceptables de gestión de la Red por parte de los ISP incluyan algún tipo de capacidad de discernimiento y bloqueo frente a determinados contenidos que pudieran ser considerados «nocivos» no ya en términos técnicos sino de legalidad. Pensemos por ejemplo en contenidos delictivos o que vulneren la legislación en materia de propiedad intelectual. Este es, ciertamente, un debate importante y actual, en la medida en que los poderes públicos, frente a las dificultades de «alcanzar» buena parte de los responsables de los contenidos que circulan en la Red, pueden sentir la tentación de acudir a la «última milla» e imponer a los ISP facultades de inspección y control que aquellos difícilmente pueden ejercer actualmente de modo directo. Creo, sin embargo, que dicha medida consistente en convertir a los ISP en garantes y controladores de la legalidad de los contenidos supone atribuir a los mismos una carga desproporcionada, tanto desde el punto de vista de su contenido como de las consecuencias lógicas de la misma: es decir, si aceptamos que los ISP no son neutrales respecto de la

5. El 22 de junio del 2011 el Parlamento de los Países Bajos aprobó una ley en virtud de la cual, entre otros aspectos, se imponía a los prestadores de servicios de comunicaciones electrónicas móviles de banda ancha no bloquear, discriminar o imponer el pago de un precio adicional en la utilización del servicio de Internet para efectuar llamadas de voz y/o imagen tipo Skype. Se trata, ciertamente, de una legislación muy avanzada respecto a la regulación existente en el resto de la Unión Europea y que contrasta vivamente con el tono cauto y genérico en el que el 19 de abril del 2011 la Comisión Europea había elaborado su Comunicación dirigida al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones sobre «The open internet and net neutrality in Europe» (Comisión Europea, 2010). Asimismo, la decisión de los Países Bajos de apostar por una regulación estricta en materia de defensa de la NN ha sido objeto de crítica por parte de la vicepresidenta de la Comisión y responsable de la Agenda Digital Europea Neelie Kroes, en la medida en que se aleja de la posición de *wait and see*, patrocinada actualmente por parte de las instituciones de la Unión.

licitud de los contenidos que transportan, deberemos entonces atribuirles algún tipo de responsabilidad en el caso de que faciliten el acceso y distribución de algún contenido ilícito. Hay que insistir en que la experiencia demuestra que este es un escenario muy tentador para los poderes reguladores, especialmente en lo que se

refiere a la protección de la propiedad intelectual. Sin embargo, resultaría claramente desproporcionado y rompería con los términos en los que hasta ahora se ha vinculado el efectivo ejercicio de libertades artísticas y expresivas con la asunción de responsabilidades jurídicas.⁶

Bibliografía

- CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION (2009). *Review of the Internet traffic management practices of Internet service providers*. 21 de octubre de 2009. <www.crtc.gc.ca/eng/archive/2009/2009-657.htm>
- COMISIÓN EUROPEA (2010). *Report on the public consultation on «The open Internet and net neutrality in Europe»*. 9 de noviembre de 2010. <ec.europa.eu/information_society/policy/ecom/doc/library/public_consult/net_neutrality/report.pdf>
- FEDERAL COMMUNICATIONS COMMISSION (2008). *Resolución sobre el caso ComCast* (FCC 08-183). 1 de agosto de 2008. <<http://cyberlaw.stanford.edu/files/blogs/FccComcastOrder.pdf>>
- FEDERAL COMMUNICATIONS COMMISSION (2010). *Report and order in the matter of preserving the open Internet broadband industry practices* (FCC 10-201). 21 de diciembre de 2010. <transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf>
- LAGUNA DE PAZ, J. C. (2009). «Internet en un cruce de caminos: ¿neutralidad o gestión razonable de las infraestructuras?» *Civitas Revista Española de Derecho Administrativo*. N.º 141, pág. 43 y sig.
- MARSDEN, C. (2010). *Net neutrality: towards a co-regulatory solution*. Londres: Bloomsbury Publishing. Disponible también en: <papers.ssrn.com/sol3/papers.cfm?abstract_id=1533428>
- PASQUALE, F. (2008). «Internet nondiscrimination principles: commercial ethics for carriers and search engines». *The University of Chicago Legal Forum*. <www.stanford.edu/dept/law/ipsc/pdf/pasquale-frank.pdf>
- WU, Tim (2003). «Net neutrality, broadband discrimination». *Journal of Telecommunications and High Technology Law*. Vol. 2, pág. 141.

6. Sobre la necesidad de pensar en nuevos esquemas regulatorios en esta materia (incluyendo aquí la llamada corregulación) resulta indispensable la lectura de la obra de Chris Marsden, *Net neutrality: towards a co-regulatory solution*.

Cita recomendada

BARATA MIR, Joan (2012). «El concepto de *net neutrality* y la tensión entre regulación pública y autorregulación privada de las redes». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la Red y otros retos para el futuro de Internet» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 13, pág. 44-52. UOC. [Fecha de consulta: dd/mm/aa].

<<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-barata/n13-barata>>

ISSN 1699-8154



Los textos publicados en esta revista están -si no se indica lo contrario- bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Acerca del autor

Joan Barata Mir

JoanBM3@blanquerna.url.edu

Doctor en Derecho por la Universidad de Barcelona. Ha sido *visiting research scholar* en la Benjamin N. Cardozo School of Law de Nueva York y secretario general del Consejo del Audiovisual de Cataluña. Actualmente es vicedecano y profesor de Derecho de la comunicación en la Facultad de Comunicación Blanquerna (URL).

Universidad Ramon Llull

Facultad de Comunicación Blanquerna

Valldonzella, 23

08001 Barcelona, España

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet»

ARTÍCULO

Privacidad en Internet y el derecho a ser olvidado/derecho al olvido

Cécile de Terwangne

Fecha de presentación: diciembre de 2011

Fecha de aceptación: diciembre de 2011

Fecha de publicación: febrero de 2012

Resumen

El derecho al olvido, también llamado derecho a ser olvidado, es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado. Internet ha traído consigo la necesidad de un nuevo equilibrio entre la libre difusión de la información y la autodeterminación individual. Este equilibrio es precisamente lo que está en juego con el derecho al olvido. Este derecho presenta tres facetas: el derecho al olvido del pasado judicial, el derecho al olvido establecido por la legislación de protección de datos y un nuevo derecho digital y aún polémico al olvido, que equivaldría a la atribución de una fecha de caducidad a los datos personales o que debería ser aplicable en el contexto específico de las redes sociales. Este trabajo analiza cada una de estas facetas en el entorno de Internet.

Palabras clave

derecho a ser olvidado, derecho al olvido, privacidad, protección de datos, derecho a objetar

Tema

Ley sobre tecnologías informáticas, Ley de protección de datos

Internet Privacy and the Right to Be Forgotten/Right to Oblivion

Abstract

The right to oblivion, equally called right to be forgotten, is the right for natural persons to have information about them deleted after a certain period of time. The Internet has brought with it a need for a new balance between the free dissemination of information and individual self-determination. This balance is precisely what is at stake with the right to oblivion. This right has three facets: the right to oblivion of the judicial past, the right to oblivion established by data protection legislation and a new, and still controversial, digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks. This paper analyses each of these facets within the Internet environment.

Keywords*right to be forgotten, right to oblivion, privacy, data protection, right to object***Topic***IT law, data protection law*

Introducción

El derecho al olvido, también llamado derecho a ser olvidado, es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado.

El desarrollo de las tecnologías de la información y la comunicación (TIC) ha sido determinante en cuanto a la ampliación del alcance de ese derecho. El progreso tecnológico ha tenido un impacto considerable en este campo. Internet -que puede ser tomado como el paradigma más representativo del cambio técnico y sociológico radical al que nos hemos enfrentado- ha traído consigo la necesidad de nuevos equilibrios entre la libre difusión de la información y la autodeterminación individual. Este equilibrio es precisamente lo que está en juego con el derecho al olvido.

La infalibilidad de la *memoria total* de Internet contrasta con los límites de la memoria humana. Ahora la memoria puede ser una memoria de rencor, venganza o menosprecio. Gracias a su «efecto eterno»,¹ Internet preserva los malos recuerdos, los errores del pasado, los escritos, las fotos o los vídeos de los que nos gustaría renegar. «La transparencia de la información sobre los errores de la trayectoria de alguien, las condenas y los estilos de vida podrían afectar y alterar la vida de otras personas relacionadas. Resulta muy fácil establecer vínculos desafortunados o injustos en Internet. Cualquiera que quiera crear problemas al prójimo o a su compañero puede usarlos».² La comisaria europea de justicia, Viviane Reding, declaró recientemente: «Como dijo alguien una vez: “Dios perdona y olvida, pero la web nunca”. Por eso, el derecho a ser olvidado es tan importante para mí. Con más y más

datos circulando por la web -sobre todo en las redes sociales- las personas deben tener derecho a que sus datos se eliminen completamente».³

Este trabajo está dedicado a la presentación y análisis de este derecho al olvido, al examen de cada una de sus facetas. Este derecho presenta en realidad tres facetas, cada una vinculada a un contexto específico. Pero, antes de pasar a estudiar estas facetas, es conveniente aclarar el significado de privacidad en Internet, que subyace a la cuestión del derecho a ser olvidado. Este concepto no siempre se descifra correctamente y una percepción inadecuada de la privacidad en Internet podría suponer un enfoque sesgado de la cuestión.

1. La privacidad en Internet

Cuando pensamos en la privacidad en Internet, la palabra *privacidad* no se debe interpretar como *intimidad* o *secretismo*. Más bien se refiere a otra dimensión de la privacidad, es decir, a la autonomía individual, la capacidad de elegir, de tomar decisiones informadas, en otras palabras, a mantener el control sobre diferentes aspectos de nuestra propia vida.

En el contexto de Internet, esta dimensión de la privacidad significa autonomía informativa o autodeterminación informativa. Internet maneja grandes cantidades de información sobre personas. Estos datos personales con frecuencia se tratan en el sentido de que se dan a conocer, se difunden, se comparten, se pueden seleccionar, descargar, registrar y usar de muchas maneras. En este sentido, la autonomía individual está en relación directa con la información personal. La libre determinación sobre la

1. Walz (1997), pág. 3.

2. Ettighoffer (2008), pág. 2 (nuestra traducción).

3. Reding (2010).

información significa tener el control sobre nuestra información personal, es decir, es el derecho de los individuos a decidir qué información sobre ellos mismos será revelada, a quién y con qué objetivo.

En Internet, nos encontramos con al menos dos dificultades. Es difícil controlar a quién se está divulgando información. Lo que hayamos decidido dar a conocer a ciertos destinatarios, ya que pertenecen a un círculo determinado (amigos, familiares, compañeros de trabajo, personas que participan en un foro, los miembros de un grupo de interés etc.) no necesariamente queremos que sea accesible a otras personas ajenas a ese círculo. Mientras que hoy en día, los motores de búsqueda como Google recogen información de diversos contextos. Al hacerlo, toman los datos de los círculos iniciales y hacen que sea muy difícil de controlar a quién se divulga la información. La otra dificultad se refiere al momento en que se produce la divulgación. Lo que se ha dado a conocer en un momento de la vida, no necesariamente queremos que esté permanentemente disponible. Esto plantea la cuestión misma del reconocimiento o no de un derecho a ser olvidado.

Antes de centrarnos en este último punto, debemos precisar un término. El concepto de información personal o datos personales debe interpretarse en un sentido amplio, ya que no debe estar vinculado a la idea de la intimidad propia de un planteamiento clásico de la privacidad. Más bien significa *cualquier* información relacionada con una persona física. Así, abarca datos profesionales, comerciales y datos hechos públicos.

En Europa, esta autodeterminación informativa ha sido reconocida y protegida como un derecho, es decir, el derecho a la protección de los datos personales. El Tribunal Europeo de Derechos Humanos ha derivado esta nueva dimensión de la privacidad del artículo 8 del Convenio europeo de Derechos Humanos.⁴ El Convenio 108⁵ del Consejo de Europa establece desde 1981 el derecho a la protección en lo que respecta al tratamiento automatizado

de los datos personales. La Carta de los Derechos Fundamentales de la Unión Europea⁶ es el primer catálogo general internacional de libertades y derechos fundamentales que menciona el derecho a la protección de datos como un derecho autónomo, protegido como tal. En su artículo 8.1 establece que: «Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan». Por último, la directiva 95/46⁷ de la Unión Europea relativa a la protección de las personas respecto al tratamiento de datos personales y a la libre circulación de tales datos ofrece un régimen jurídico muy detallado.

2. El derecho al olvido del historial judicial

2.1. El criterio de interés periodístico o de interés histórico

La primera faceta del derecho al olvido está relacionada con el pasado judicial o penal de un individuo. Es la faceta más clásica. Inicialmente estaba vinculada sobre todo a la creación de registros de antecedentes penales. Hoy en día, el derecho al olvido del historial judicial ha ido mucho más allá de los antecedentes penales. La jurisprudencia de varios países lo ha reconocido, basándose en el derecho a la privacidad o como parte de los derechos de la personalidad. Está justificado por la fe en la capacidad del ser humano de cambiar y mejorar, así como en la convicción de que el ser humano no debe reducirse a su pasado. Una vez pagado lo debido, la sociedad debe ofrecerle la posibilidad de rehabilitarse e iniciar una nueva vida sin tener que soportar el peso de sus errores del pasado el resto de su vida.

Este derecho entra en conflicto con el derecho a la información; el tiempo es el criterio para resolver el conflicto. El derecho al olvido debe dar prioridad a las exigencias del derecho a la información cuando los hechos que se revelan presentan un interés específico para su divulgación.

4. Véanse, entre otros, E.Ct.H.R., *Rotaru v. Romania*, 4 mayo 2000, appl. no 28341/95, § 43; *Amann v. Switzerland*, 16 febrero 2000.
5. Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ETS n.º 108, 28.1.1981).
6. Carta de los derechos fundamentales de la Unión Europea, *Diario oficial*, 18 diciembre 2000, C-364/1.
7. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario oficial*. L 281, 23/11/1995, pág. 31-50.

El interés está vinculado, por tanto, al interés periodístico de los hechos. Esto sucede cuando una decisión judicial pronunciada por un tribunal forma parte de las noticias judiciales. Es entonces legítimo recordar esta decisión mencionando los nombres de las partes (excepto si son menores de edad, en cuyo caso se aplican diferentes normas de protección). Pero con el transcurso del tiempo, cuando ya no se trata de una cuestión de actualidad o noticiable, y siempre y cuando ya no exista una razón que justifique una nueva divulgación de la información como noticia, el derecho al olvido anula el derecho a la información. Aún se puede mencionar el caso, pero no se deben incluir los nombres de las partes o los datos identificados. Por lo tanto, el valor informativo de un caso inclina la balanza a favor del derecho a difundir a costa del derecho al olvido. Y en cuanto deja de tener valor como noticia, la balanza se inclina en la otra dirección.

Se pueden admitir dos excepciones. Esto significa que el derecho a la información anulará el derecho al olvido a pesar del tiempo transcurrido:

- para los hechos relacionados con la historia o cuando se trate de un tema de interés histórico y
- para los hechos vinculados al ejercicio de la actividad pública por parte de una figura pública.

El interés histórico y el interés público también se deben tener en cuenta para resolver el conflicto entre el derecho al olvido y el derecho a la información.

2.2. El impacto de los desarrollos técnicos

2.2.1. La recogida de información: el poder de los motores de búsqueda

Los avances técnicos han cambiado radicalmente el equilibrio alcanzado entre la necesidad de divulgar la información judicial y el derecho individual a ser olvidado. Como ya hemos mencionado, la información más insignificante puede sacarse a la luz pública y añadirse a otra información. Esto implica un cambio radical. Vale

la pena citar una decisión del Tribunal Supremo⁸ de los Estados Unidos pronunciada hace más de veinte años, pero muy esclarecedora incluso hoy, en la que el Tribunal Supremo subrayó el cambio. El caso se refería a un periodista que había solicitado acceso a los documentos del FBI relacionados con las condenas de cuatro personas. Tres de ellas habían muerto y el FBI se negó a revelar datos de la cuarta que se habían guardado en un formato compilado, aduciendo que se vulneraría la intimidad de esta persona. El Tribunal Supremo confirmó por unanimidad esta decisión, en contra del Tribunal de Apelación que había declarado que ya no había interés de privacidad, ya que la información había sido publicada. El Tribunal Supremo dictaminó lo siguiente: «Pero el tema aquí es si la compilación de información, que de otro modo sería difícil de obtener, altera el interés de privacidad implicado por la divulgación de esa información. Es evidente que hay una gran diferencia entre los archivos públicos que se pueden encontrar después de una diligente búsqueda de los registros de los tribunales de justicia, los archivos del condado y las comisarías de policía de todo el país y un resumen computarizado guardado en un centro único de información». ⁹ En el mismo sentido, un tribunal de apelaciones de California declaró que «es la naturaleza global de la información la que la hace valiosa para el demandante; es la misma calidad que hace su difusión constitucionalmente peligrosa». ¹⁰

La potencia de los motores de búsqueda de Internet para recopilar datos relativos a un individuo concreto en cualquier momento, desde cualquier lugar, sin ningún tipo de procedimiento administrativo, sin que la persona que los busca revele su identidad propia y de forma gratuita plantea un peligro aún mayor. Debemos repensar cuidadosamente el equilibrio necesario. Sobre el tema concreto de los datos sobre el pasado judicial, una primera respuesta es imponer el anonimato en las bases de datos de jurisprudencia disponibles en Internet. ¹¹ Esa imposición del anonimato es ahora la regla en la mayoría de los países europeos. Sin embargo, otro asunto importante es la cuestión de los archivos de los periódicos. Este problema será analizado a continuación.

8. *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).

9. 489 U.S., 764.

10. *Westbrook v. Los Angeles County*, 32 Cal. Rptr. 2d 382 (Cal. App. 1994).

11. Sobre esta cuestión, que no podemos desarrollar con mayor profundidad en este artículo, véase De Terwangne (2005), pág. 40-48.

2.2.2. La disponibilidad eterna de la información: el caso de los archivos de periódicos en Internet

Los archivos de periódicos en Internet son una fuente de información de todo tipo de lo que alguna vez fueron noticias. Muchas de esas noticias hablan de personas. No se limitan a datos judiciales, claro. Aunque nos centramos en esto último, lo que se dice a continuación es válido también para cualquier otra información personal.¹²

Los datos judiciales mencionados en un periódico quedan eternamente accesibles en su archivo electrónico. Esto plantea el problema de un posible conflicto entre el derecho de la persona juzgada a ser olvidado (sobre la base del derecho a la privacidad, los derechos de la personalidad o el derecho al libre desarrollo de la personalidad) y la libertad de la prensa.

No existe *a priori* una jerarquía entre los derechos humanos, lo que significa que los conflictos entre derechos no se pueden resolver dando prioridad sistemática a un derecho sobre otro. Resolver un conflicto siempre requiere realizar una ponderación entre los derechos implicados para poder alcanzar un equilibrio. El perjuicio que experimente el valor sacrificado no debe guardar excesiva desproporción respecto al beneficio obtenido por el otro valor en conflicto.

En cuanto al conflicto planteado por los archivos de periódicos en Internet, se deben tener en cuenta los criterios antes mencionados de interés periodístico, de interés histórico y de interés público. Por definición se considera que la información contenida en los archivos de los periódicos ya no tiene un interés periodístico. Al considerar el valor histórico de los hechos, se debería tener especialmente en cuenta si hay otras fuentes de información. En cuanto a los datos judiciales, se debe prestar atención especial en cuanto a si se han apelado las decisiones judiciales guardadas en los archivos de los periódicos. Si es así, la primera sentencia podría mantenerse, pero debería ir acompañada de una nota que indicara que la decisión se encuentra pendiente de revisión.

En el caso reciente de *Times Newspapers*, el Tribunal Europeo de Derechos Humanos dio unas indicaciones muy interesantes relativas a cómo debe realizarse la ponderación. Aunque el derecho al olvido no estaba en juego en este caso,¹³ la decisión del Tribunal podría aplicarse de manera útil a las hipótesis que implican un conflicto entre la libertad de la prensa y el derecho al olvido como sucede en los casos de archivos de periódicos accesibles al público. El tribunal declaró que mantener archivos es de gran interés para la sociedad, pero constituye sin embargo un papel secundario de la prensa. En consecuencia, este aspecto de la libertad de prensa tiene menos peso, a la hora de realizar una ponderación, que si estuviera en juego la función principal de información que le corresponde. El Tribunal declaró que estaba «de acuerdo inicialmente con las alegaciones del demandante en cuanto a la importante contribución hecha por los archivos de Internet para conservar y mantener noticias e información disponibles. Estos archivos constituyen una fuente importante para la educación y la investigación histórica, sobre todo porque son fácilmente accesibles al público y son generalmente gratuitos. El Tribunal considera que, aunque la función principal de la prensa en una democracia es la de actuar como un 'perro guardián', tiene un valioso papel secundario en el mantenimiento y puesta a disposición del público de los archivos que contienen noticias que ya se han publicado. Sin embargo, el margen de apreciación de que disponen los Estados para lograr el equilibrio entre derechos es probable que sea mayor en lo que se refiere a archivos de noticias de acontecimientos pasados que en lo referente a la transmisión de noticias de actualidad. [...]»¹⁴

Por tanto, se puede prever que el resultado de la ponderación necesaria sea que se deben borrar los datos de identificación de un artículo guardado en los archivos de un periódico en Internet. Sin embargo, siempre se debe llegar a una conclusión analizando el tema caso por caso. Debe tenerse en cuenta que este problema se halla estrechamente relacionado con el acceso público a la información controvertida a través de Internet. El equilibrio alcanzado en lo que se refiere a la disponibilidad en Internet no se corresponde

12. Otro artículo de este número de la revista trata la cuestión del derecho al olvido y la prensa, y por lo tanto estudia más a fondo los problemas relacionados con los archivos de los periódicos.

13. Se trataba de una cuestión de presunta difamación vinculada a la información mantenida en los archivos de Internet de *The Times*; los artículos originales se habían presentado sin advertencia previa de que habían sido objeto de una demanda por difamación.

14. E.Ct. H.R., *Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom*, 10 marzo 2009, appl. no. 3002/03 y no. 23676/03, § 45 (el énfasis es nuestro).

necesariamente con lo que se debe hacer en el caso de los formatos clásicos. Es muy probable que ciertas soluciones consistan en dar prioridad al derecho al olvido en lo que se refiere a archivos en Internet, mientras que se dé prioridad a la libertad de la prensa, los intereses históricos, educativos y públicos de los archivos en formatos no accesibles a través de Internet. El daño que se deriva de la disponibilidad eterna y universal de los datos en Internet se considerará con mucha mayor frecuencia una medida desproporcionada que el daño resultante de un centro de información local con acceso controlado por procedimientos.

3. El derecho al olvido establecido por la legislación de protección de datos

Como ya se ha señalado, los avances tecnológicos han dado lugar a la multiplicación de los usos de los datos y de los lugares donde los datos se almacenan y tratan. Las herramientas electrónicas se han vuelto más y más poderosas, presentando cada vez más capacidad de almacenamiento y una extraordinaria eficacia en la selección y la recuperación de información. Han aparecido leyes de protección de datos, no para inhibir el progreso técnico, sino para ofrecer un marco a los nuevos desarrollos para volver a equilibrar las cosas.

La segunda faceta del derecho al olvido se deriva de esa reglamentación de la protección de datos. Mediante diferentes principios, esta legislación garantiza lo que se puede considerar como un derecho a ser olvidado. Pero en este contexto, el derecho al olvido se amplía. Ya no se vincula exclusivamente al pasado judicial, sino que se aplica al tratamiento de cualquier dato personal.

Antes de detallar los principios que dan forma a este derecho, vale la pena precisar que no existen instrumentos globales jurídicamente vinculantes en materia de protección de datos.¹⁵ Las legislaciones nacionales y algunos instrumentos regionales abordan el tema.¹⁶ Entre ellos, la Directiva 95/46 de la Unión Europea¹⁷ presenta un interés indudable ya que es el régimen de protección aprobado más detallado. Por esta razón, se hace referencia a ese instrumento jurídico en los párrafos siguientes. Pero aparte de su interés como configuración legal de un derecho a ser olvidado, hay que tener en cuenta que este régimen europeo no es, sin embargo, una respuesta global a las cuestiones planteadas en el universo de Internet.

3.1. La obligación de eliminar o hacer anónimos los datos personales derivada del principio de finalidad

Uno de los principios básicos del régimen de protección de datos es el principio de finalidad. Este principio establece que los datos personales se deben tratar con un objetivo determinado, legítimo y transparente. El derecho al olvido se deriva directamente del principio de finalidad, ya que, de acuerdo con una aplicación de este principio, el responsable del tratamiento de los datos puede mantener los datos personales «en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente».¹⁸ Esto significa que los datos personales se pueden mantener como tales si la finalidad del tratamiento lo justifica. Se deben hacer anónimos o se deben eliminar una vez que el objetivo se ha logrado o cuando ya no sea necesario mantener el vínculo con personas identificables para lograr ese propósito.

Esta norma establece claramente el derecho al olvido. Como mínimo, la legislación de protección de datos obliga

15. La Resolución de Madrid adoptada por un colectivo de agencias nacionales de protección de datos no es más que una propuesta en este momento y no es legalmente vinculante. Véase Agencia Española de Protección de Datos (2009).

16. Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ETS n.º 108, 28.1.1981). Directrices de la OCDE sobre la protección de la vida privada y los flujos transfronterizos de datos personales, publicadas en www.oecd.org; APEC Privacy Framework, noviembre 2004 (http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html).

17. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario oficial*. L 281, 23/11/1995, pág. 31.

18. Art. 6, § 1, e) de la directiva 95/46.

a cualquier persona que trate datos personales a prever y respetar una fecha de caducidad de estos datos.

Los interesados tienen derecho a comprobar que esta regla se respeta.¹⁹ Se les concede el derecho a que el responsable del tratamiento de los datos suprima o bloquee los datos cuyo tratamiento no se ajuste a las limitaciones derivadas del principio de finalidad.

Además, se pueden imponer sanciones si se infringe la regla.²⁰

3.2. Atenuación del derecho a ser olvidado

Los autores de la directiva sobre protección de datos eran conscientes de que en muchos casos los que llevan a cabo investigación histórica, científica o estadística tienen que usar datos que no se habían recogido inicialmente para ese propósito. Con el convencimiento de que este tipo de investigación es importante para la sociedad, se optó por un sistema que admite sistemáticamente el uso histórico, científico o estadístico de los datos condicionado a que los estados establezcan las garantías apropiadas para tales usos.²¹

Esto significa que los datos personales se pueden mantener después de su fecha de caducidad si esos fines específicos lo justifican. Las garantías nacionales varían de un estado a otro. Ciertos estados han previsto la obligación de anonimizar los datos o por lo menos codificarlos. Mantener los datos en su forma original debe estar justificado. Sin embargo, otras medidas de seguridad nacional son más minimalistas.

Otra especificidad de la legislación de protección de datos supone una atenuación del derecho al olvido. El artículo 9 de la directiva 95/46, estipula un régimen de

exención para el tratamiento de datos con fines periodísticos²² o con fines relacionados con la expresión artística o literaria. Los estados miembros están invitados a definir las excepciones apropiadas que consideren necesarias para «conciliar el derecho a la privacidad con las normas que rigen la libertad de expresión».²³ En función de las derogaciones que hayan sido reconocidas por un Estado, quienes traten datos personales para estas finalidades pueden verse liberados de la obligación de borrar los datos una vez la finalidad ha sido alcanzada.

3.3. El derecho a oponerse al tratamiento de datos personales

Para beneficiarse del derecho a ser olvidado que deriva del principio de finalidad, el interesado no tiene que hacer nada. Es el responsable del tratamiento quien tiene la responsabilidad de asegurarse de que los datos personales se borran cuando se cumple el propósito del tratamiento. La directiva establece otra forma de hacer cumplir el derecho a ser olvidado. Esta vez, la iniciativa corre a cargo del titular de los datos.

Según el artículo 14 de la Directiva 95/46, los sujetos cuyos datos sean tratados tienen derecho a oponerse «en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento [...]. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos». Cuando el tratamiento de los datos se hace con fines de marketing directo, el derecho a objetar no necesita ningún tipo de justificación.²⁴

Frente al alboroto creado por los medios de comunicación en torno a la reciente afirmación de garantizar a cualquiera un derecho digital al olvido, se dijo que lo que se

19. Art. 12 de la directiva 95/46.

20. Art. 24 de la directiva 95/46.

21. Lo mismo se acepta para fines estadísticos y científicos, véase el artículo 6 § 1, b), *in fine*, de la directiva 95/46: «no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembro establezcan las garantías oportunas».

22. Para entender lo que significa un fin periodístico, véase la importante decisión del Tribunal Europeo de Justicia en el caso *Satamedia*: E.C.J., 16 de diciembre de 2008, *Satakunnan Markkinapörssi Oy y Satamedia Oy*, Case C-73/07. Véase también De Terwangne (2010), nota bajo E.C.J., 16 diciembre 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy*, Case C-73/07, R.D.T.I., n.º 38, págs. 132-146.

23. Art. 9, *in fine*, de la directiva 95/46.

24. Art. 14, § 1, b) de la directiva 95/46.

reivindicaba era tal vez simplemente la traducción «lírica» del derecho a oponerse que ya existía.²⁵

Vale la pena señalar que este derecho de oposición no es totalmente equivalente a un derecho a eliminar los datos personales propios. Esto equivale a un derecho a suspender el tratamiento de los datos en cuestión. En muchos casos, esto significará borrar los datos, ya que tratarlos implica almacenarlos. Pero no siempre será así. En el sector de marketing directo, por ejemplo, el titular de los datos que se oponga al marketing directo por teléfono será puesto en una lista especial de personas cuyo número de teléfono no se puede usar para fines de marketing directo (llamada, por ejemplo, *lista naranja* o *lista de Robinson*).

No respetar la objeción de tratamiento basada en razones legítimas es sancionable.

4. Reivindicación de un nuevo derecho digital al olvido

Recientemente, el derecho a ser olvidado ha sido el centro de intensos debates, de los que se ha informado en la prensa, en informes oficiales, en declaraciones políticas, en blogs etc. La controversia es acerca de la conveniencia de ampliar el actual derecho a ser olvidado en respuesta a las situaciones creadas por la mejora del entorno de Internet. Según el presidente de la Comisión Nacional de Informática y Libertades (CNIL) francesa, lo que está en juego con este replanteamiento del derecho al olvido es encontrar de nuevo una función natural -olvidar- que haga la vida soportable.²⁶

4.1. El contexto de la reivindicación: las particularidades de Internet

El nuevo derecho al olvido digital reivindicado está claramente vinculado a determinadas particularidades de Internet. Ya se han mencionado algunas de estas particularidades: el *efecto eterno* de la memoria electrónica,

así como la eficiencia de los motores de búsqueda para encontrar en Internet los datos más insignificantes, fuera de su contexto original, y reunir todos los datos para ofrecer un retrato recompuesto, aunque muchas veces heterogéneo. Vinculado a la *memoria absoluta* de Internet, este retrato puede consistir en características pasadas eternamente presentes y, a veces, puede ser perjudicial. De hecho, han aparecido empresas especializadas en el manejo de la *e-reputación* de las personas físicas y jurídicas en Internet. Ofrecen realizar operaciones de limpieza puntuales o a largo plazo para proteger, mantener o restaurar la reputación y la propia imagen.

Otra particularidad es que, contrariamente a lo que sucede en la vida física, la eliminación de datos en el mundo digital exige tomar una decisión al respecto. Se trata de un proceso consciente y voluntario. Hay que tener la voluntad de eliminar los datos.

Además, se ha vuelto menos costoso almacenar los datos que eliminarlos o hacerlos anónimos. De hecho, las capacidades de almacenamiento han crecido exponencialmente, mientras que sus costes se han reducido. «Por lo tanto, ejercer los derechos de la personas va en contra de la tendencia natural de la economía».²⁷

4.2. El derecho a la eliminación automática de los datos en el entorno electrónico

Como respuesta a los nuevos desarrollos de los servicios de Internet y a la problemática situación que se deriva de las particularidades de Internet señaladas, se ha hecho la misma proposición en diferentes círculos políticos, institucionales o de expertos para conceder a los titulares de datos personales un derecho automático a ser olvidados transcurrido un plazo determinado. Concretamente, el Supervisor europeo de protección de datos ha propuesto ampliar el derecho consolidado a ser olvidado para garantizar que los datos desaparezcan automáticamente después de un cierto período de tiempo, incluso aunque los titulares interesados no tomen medidas o no sean conscientes de que se hayan

25. Cyberlex (2010), pág. 10.

26. Turk (2009).

27. Supervisor Europeo de Protección de Datos (2011).

guardado sus datos personales.²⁸ El secretario general adjunto del Consejo de Europa llegó a la misma conclusión: «El aumento de la capacidad de almacenamiento y de tratamiento permite que la información sobre una persona circule por Internet aunque ya no sea válida. Esto hace obsoletos los principios actuales de exactitud y proporcionalidad de los datos. *Un nuevo derecho al olvido o a la eliminación automática de los datos* permitiría que las personas tomaran control sobre el uso de sus datos personales».²⁹ Por su parte V. Reding, vicepresidenta de la Comisión Europea, dijo: «Quiero introducir el *derecho a ser olvidado*. Los entornos de redes sociales son una buena manera de mantenerse en contacto con los amigos y compartir información. Pero si las personas ya no quieren usar un servicio, no deberían tener problemas para borrar sus perfiles. El derecho a ser olvidado es particularmente relevante respecto a los datos personales que ya no son necesarios para los fines para los que se habían recogido. Este derecho también se debería aplicar cuando haya transcurrido un período de almacenamiento aceptado por el titular de los datos.»³⁰

Estas propuestas similares equivalen a atribuir una fecha de caducidad a los datos sin necesidad de un análisis previo caso por caso. Se podría fijar un período de tiempo determinado, por ejemplo, para los datos almacenados en ciertos equipos, como los teléfonos móviles o los ordenadores: los datos se eliminarían o bloquearían automáticamente después de un período de tiempo determinado si esos equipos ya dejasen de estar en poder de sus iniciales propietarios.

Este sistema ya se aplica en algunos estados para ciertos archivos o registros, como los de la policía judicial. Esto afirma lo que el Tribunal Europeo de Derechos Humanos ha subrayado en el caso *Rotaru*: los datos relativos al pasado distante de un individuo plantean un problema especial en cuanto a la *vida privada* protegida por el artículo 8, párrafo 1 del Tribunal Europeo de Derechos Humanos. Los datos no deben mantenerse sin un análisis muy estricto de su necesidad en cuanto a requisitos democráticos.³¹

La automaticidad de la eliminación o prohibición de uso ulterior se debería traducir en una configuración de *privacidad por defecto* en el tratamiento de los datos personales. En este sentido, el derecho al olvido podría convertirse en una obligación a la *privacidad por diseño*. Una respuesta técnica así podría contribuir a inclinar la balanza a favor de los titulares de los datos personales ya que estos últimos se beneficiarían de la protección sin tener que tomar ninguna iniciativa. Esto es particularmente importante en un contexto tan opaco como Internet. Los titulares de los datos personales no son conscientes de muchos tratamientos de datos que se producen en este ámbito. En ese caso, es ilusorio para garantizar a los individuos un derecho que nunca se les ocurriría ejercer.

Observamos que *olvidar* podría significar obligar a eliminar los datos, pero también podría significar preferentemente prohibir seguir usando los datos, al menos en el formato personalizado. Tal vez esto sería más realista, si tenemos en cuenta el coste económico de eliminar los datos ya mencionado. Si nos centramos en los problemas específicos de los medios de comunicación en Internet y las redes sociales, *olvidar*, también podría equivaler a prohibir seguir difundiendo los datos.

4.3. El derecho a hacer que la información sea eliminada y no solo inaccesible

Ha aparecido un problema específico en el entorno de las redes sociales. Ciertas redes sociales se han mostrado renuentes a eliminar datos después de que el titular que los puso en una página de la red social decidiera darse de baja de este servicio. Generalmente, el servicio cumple con la decisión de no publicar más los datos, pero se niega a destruirlos. En respuesta a esta dificultad, algunas voces consideraron la posibilidad de establecer un derecho a hacer que la información propia se elimine y no solo que sea inaccesible.

Esto estaría especialmente reservado para los casos en los que la información ha sido divulgada por iniciativa del

28. Supervisor Europeo de Protección de Datos (2011), § 85.

29. Consejo de Europa, Secretario general adjunto (2010) (el énfasis es nuestro).

30. Reding (2010) (el énfasis es nuestro).

31. E.Ct.H.R., *Rotaru v. Romania*, 4 mayo 2000, appl. no 28341/95. Véase también la opinión concurrente del juez Wildhaber a la que se adhieren los jueces Makarczyk, Türmen, Costa, Tulkens, Casadevall y Weber.

titular. Esta solución le parece bastante lógica y evidente a Peter Fleisher, aunque es un ferviente opositor al derecho al olvido. Según él, «Si divulgo algo en Internet ¿debería tener el derecho a borrarlo? Creo que la mayoría de nosotros estaría de acuerdo con ello, como caso más simple y menos controvertido. Si publico una foto en mi álbum, debería poder eliminarla después si cambio de idea».³²

4.4. Una difícil aplicación práctica

Debemos ser conscientes de los límites técnicos de la aplicación del derecho a ser olvidado. Conseguir que nuestros datos se eliminen de Internet no es tan fácil.³³ Primero hay que solicitar al editor del sitio web en cuestión que elimine los datos problemáticos. Después de que el editor haya accedido a la solicitud, la información seguirá estando disponible en los resultados presentados por los motores de búsqueda en la memoria caché durante un tiempo.³⁴ La siguiente indexación del sitio web puede tardar unos días o semanas antes de que la nueva versión sustituya a la anterior en la memoria caché. Durante todo el tiempo que los datos hayan sido de dominio público, las personas interesadas en la información pueden haberla descargado y divulgado. Es algo que nunca sabremos con certeza. Si descubriéramos que de una forma u otra (porque los que hubieran descargado la información la hubieran vuelto a publicar en su sitio web, por ejemplo) tendríamos que volver a repetir el proceso de limpieza. Y en algún momento de nuestra actividad sísmica, es probable que nos encontráramos o con grandes dificultades para convencer al editor de la página web o con la inercia de nuestro interlocutor. Además, la arquitectura de los sistemas informáticos se ha vuelto mucho más compleja. La multiplicación de vínculos hace cualquier eliminación de datos difícil y costosa.³⁵

Un caso reciente en el que las autoridades españolas de protección de datos establecieron una estrategia para eludir la dificultad ilustra los problemas relacionados con las operaciones de eliminación de datos. En enero de 2011, la Agencia Española de Protección de Datos ordenó a Google que retirara de sus resultados ciertos enlaces a páginas web que contenían datos personales de ciudadanos españoles. Algunos enlaces llevaban a artículos de periódicos que contenían información que podía dañar la reputación de las personas afectadas. En particular, un cirujano plástico que había estado implicado en un caso de negligencia médica en 1991 quería que Google retirase los artículos de los resultados de búsqueda relacionados con su nombre. Las autoridades españolas sostenían que presentar una orden judicial contra los motores de búsqueda como Google era la única manera de bloquear el acceso al material sensible publicado en Internet, ya que los periódicos legalmente pueden negarse a cumplir con peticiones presentadas de forma más informal.³⁶ Sin embargo, Google se negó a obedecer la orden de la Agencia Española de Protección de Datos alegando que, en su opinión, equivalía a censurar sus resultados. El caso se presentó ante un tribunal de Madrid que lo remitió al Tribunal Europeo de Justicia. Se pide al tribunal que determine si una agencia nacional de protección de datos tiene derecho a exigir la eliminación de los vínculos de los resultados presentados por un motor de búsqueda.

Por último, como último punto sobre las dificultades concretas para aplicar el derecho al olvido en Internet, debe aclararse qué datos pueden ser objeto de este derecho al borrado. ¿Solo los datos obtenidos del titular de los datos o también los datos analíticos o metadatos creados por el responsable del tratamiento?³⁷

32. Fleisher (2011).

33. En el mismo sentido, véase Cyberlex (2010), *op. cit.*, pág. 41; Fleisher (2011) *op. cit.*; Privacy International (2011).

34. Google presenta sus vínculos en caché de la siguiente manera: «Google toma una instantánea de cada página examinada mientras explora la web y la guarda en caché como copia de seguridad en caso de que la página original no esté disponible. Si hace clic en el vínculo "Caché", verá la página web como se veía cuando fue indexada. El contenido caché es el contenido que Google usó para juzgar si la página es una buena coincidencia para su búsqueda. La página almacenada en caché se mostrará con un encabezado que recuerda que se trata de una versión caché de la página y no la propia página.» Disponible en : http://www.google.com/intl/en/help/features_list.html#cached (traducción del editor).

35. Cyberlex (2010), pág. 33.

36. Halliday (2011); "Spain demands the right to oblivion for its citizens", *Law and the Internet*, blog del bufete de abogados Finocchiaro, 31 Marzo 2011; Gómez (2011).

37. De Terwangne y Moyné (2011), pág. 22-23.

4.5. Una dificultad derivada del modelo económico de Internet

Uno de los objetivos del derecho al olvido son los rastros que los internautas dejan inconscientemente mientras circulan por Internet. Relacionados con las *cookies*, la retención de direcciones IP, los análisis de actividad en Internet, el almacenamiento de las solicitudes de búsqueda en los motores de búsqueda etc, todos estos datos son muy valiosos desde un punto de vista económico. Mantener durante mucho tiempo todas estas huellas inconscientes es fundamental para las empresas de Internet debido al modelo económico de la oferta de servicios en Internet. La mayoría de los productos o servicios de información son aparentemente gratuitos, mientras sean financiados por la publicidad individualizada y publicidad comportamental, lo que sin duda limita la posibilidad de borrar dicha información.

4.6. Intereses en conflicto

Como ya hemos mencionado respecto al derecho a olvidar el pasado judicial, el derecho al olvido entra en conflicto con otros importantes derechos, libertades e intereses legítimos. En particular, entra en conflicto con la libertad de expresión y la libertad de prensa. Incide en la conservación de archivos completos, que hemos desarrollado en el punto 2.2.2 del presente artículo en relación con los archivos de los periódicos en Internet. Por la misma razón, perjudica la obligación de recordar. Es un obstáculo para la investigación histórica. Tiene también un impacto en la continuidad de las empresas, en la gestión de expedientes de trabajadores, el deber de guardar pruebas etc.³⁸ E inevitablemente tenemos que tener en cuenta la obligación de conservar datos para fines de seguridad pública.

La Asociación Profesional Española de Privacidad lo expresa de una forma ligeramente diferente, presentando el problema como un dilema. En opinión de esta asociación, a diferencia del derecho a oponerse, el derecho a ser olvidado tiene un efecto retroactivo. Por tanto, la pregunta es si los individuos deben ser responsables de sus acciones pasadas *sine die* o si es conveniente tener el derecho a reescribir su pasado y, en consecuencia, el de los demás.³⁹

38. *Ibidem*.

39. Asociación Profesional Española de Privacidad (2011).

La respuesta a este tipo de conflictos o dilemas se encuentra de nuevo en la aplicación del principio de ponderación y respetando el principio de proporcionalidad (consulte el anterior punto 2.2.2).

Conclusión

El derecho a ser olvidado en lo que respecta al pasado penal y judicial ha sido reconocido por la jurisprudencia basándose en el derecho a la privacidad o en los derechos de la personalidad. En el entorno de Internet, este derecho podría ser una respuesta apropiada a los problemas planteados por la memoria electrónica eterna (la creación del *efecto eterno*) combinados con la potencia de la recuperación y recopilación de datos de los motores de búsqueda. El presente trabajo aborda estos problemas estudiando los ejemplos de jurisprudencia penal disponibles gratuitamente en Internet y los archivos de periódicos también públicamente disponibles en Internet. El derecho al olvido no es absoluto y debe dar prioridad a la libertad de expresión, la libertad de prensa, el derecho a la información pública o el interés público en la investigación histórica cada vez que la ponderación entre los derechos en conflicto lo exija.

Las leyes de protección de datos reconocen y protegen legalmente un derecho más amplio al olvido, que no se reduce solo a la información judicial. Es válido para cualquier dato personal, no se limita a datos privados o confidenciales. Observamos que la legislación de protección de datos ha establecido un régimen muy equilibrado en lo que se refiere al derecho al olvido. Se basa en dos principios básicos: la obligación de borrar o hacer anónimos los datos personales una vez se ha logrado el objetivo del tratamiento y el derecho concedido al titular a oponerse justificadamente al tratamiento de sus datos.

Más allá de este derecho bien establecido a ser olvidado, se reivindica un derecho aún más amplio al olvido. Está pensado para ser específicamente aplicable al entorno digital de Internet. Significaría la eliminación automática de los datos, sin que el interesado tuviera que dar ningún paso para obtener ese resultado. Equivaldría a atribuir una fecha de caducidad a los datos sin necesidad de un

análisis previo caso por caso. En este sentido, el derecho al olvido podría convertirse en una obligación a la *privacidad por diseño*. El derecho a obtener la eliminación completa de nuestros datos también se reivindica para los datos que hemos decidido revelar, lo que tiene como objetivo específico el universo de las redes sociales.

Sin embargo, la aplicación del derecho al olvido se encuentra con dificultades prácticas. Y ese derecho inevitablemente entra en conflicto con otros derechos, libertades e intereses legítimos. Una vez más, en este caso, la ponderación entre los derechos implicados y el respeto al

principio de proporcionalidad debería ofrecer la respuesta acerca de qué derecho debe prevalecer.

La cuestión de la ampliación del derecho a ser olvidado es todavía un tema controvertido. O bien las proposiciones están muy delimitadas y presentan el riesgo, si se aplican en la legislación de protección de datos, de proporcionar respuestas muy concretas a cuestiones específicas de tecnología, lo cual no es garantía de una legislación duradera o la ampliación plantea problemas por la restricción que crea a la libertad de expresión, al derecho a la información pública y al interés histórico y pedagógico.

Referencias bibliográficas

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009). *Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid*.
<http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf>
- ASOCIACIÓN PROFESIONAL ESPAÑOLA DE PRIVACIDAD (2011). «Response to the Council of Europe consultation on the modernisation of Convention No. 108». En: *Compilation of comments received on the consultation on the modernisation of Convention 108*.
<http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01mosRev6.pdf>
- ASSEMBLEE NATIONALE (France) (2011). *Révolution numérique et droits de l'individu: pour un citoyen libre et informé*. Rapport d'information par la mission d'information commune sur les droits de l'individus dans la révolution numérique.
- CONSEJO DE EUROPA, SECRETARIO GENERAL ADJUNTO (2010). «Speaking points for the opening of the 21st T-Pd bureau meeting». Estrasburgo: 15 noviembre 2010.
<<http://www.coe.int/t/dghl/standardsetting/dataprotection/151110%20DSG%20speaking%20notes%20data%20protection%20meeting%20T-PD.pdf>>
- CYBERLEX, L'Association du Droit et des Nouvelles Technologies (2010). «Contribution dans le cadre des travaux sur le droit a l'oubli numérique. L'oubli numérique est-il de droit face à une mémoire numérique illimitée?»
<http://www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf>
- DE TERWANGNE, C. (2005). «Diffusion de la jurisprudence via Internet dans les pays de l'Union Européenne et règles applicables aux données personnelles». *Petites Affiches*. N.º 194, pág. 40-48.
- DE TERWANGNE, C.; MOINY, J.-Ph. (2011). *Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data*. Estrasburgo: Consejo de Europa. T-PD-BUR(2011)10en, pág. 22-23.
<http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_en.pdf>
- DUASO-CALÈS, R. (2002). *La protection des données personnelles contenues dans les documents publics accessibles sur Internet: le cas des données judiciaires*. Memoria. Montreal: Facultad de Derecho, Universidad de Montreal.

- ESCOFFIER, A. M.; DETRAIGNE, Y. (2009). *Rapport d'information sur la vie privée à l'heure des mémoires numériques*.
 <<http://www.senat.fr/noticerap/2008/r08-441-notice.html>>
- ETTIGHOFFER, D. (2008). «Les droits de l'homme numérique: le droit à l'oubli».
 <<http://www.ettighoffer.com/fr/idees/idees8.html>>
- FLEISHER, P. (2011). «Foggy thinking about the right to oblivion». Blog de Peter Fleisher. 9 marzo 2011.
- GÓMEZ, R. G. (2011). «Google niega a Protección de Datos legitimidad para ordenar la cancelación de contenidos». *El País*, 19 enero 2011.
 <http://www.elpais.com/articulo/sociedad/Google/niega/Proteccion/Datos/legitimidad/ordenar/cancelacion/contenidos/elpeputec/20110119elpepusoc_5/Tes>
- HALLIDAY, J. (2011). «Europe's highest court to rule on Google privacy battle in Spain». *The Guardian*, 1 marzo 2011.
 <<http://www.guardian.co.uk/>>
- PRIVACY INTERNATIONAL (2011). «Response to the Council of Europe consultation on the modernisation of Convention No. 108». En: *Compilation of comments received on the consultation on the modernisation of Convention 108*. Junio 2011.
 <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01mosRev6.pdf>
- REDING, V. (2010). «Why the EU needs new personal data protection rules?» En: *The European Data Protection and Privacy Conference*. Bruselas, 30 noviembre 2010.
 <<http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700>>
- «Spain demands the right to oblivion for its citizens». *Law and the Internet*, blog del bufete de abogados Finocchiaro. 31 marzo 2011.
 <<http://www.blogstudiolegalefinocchiaro.com/wordpress/?tag=the-agencia-espanola-de-proteccion-de-datos-aepd>>
- SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (SEPD) (2011). *Dictamen sobre la comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - «Un enfoque integral sobre protección de datos personales en la Unión Europea»*. 14 enero 2011, § 85.
- TURK, A. (2009). «La délicate question du droit à l'oubli sur Internet». Entrevista en *Le Monde*, 12 noviembre 2009.
- WALZ, S. (1997). «Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society». En: *19th International Data Protection Commissars Conference*. Bruselas: 17-19 septiembre 1997.
- WERRO, F. (2009). «The right to inform v. the right to be forgotten: A transatlantic clash». En: A. COLOMBI CIACCHI; Ch. GODT; P. ROTT; L. J. SMITH (eds.). *Liability in the Third Millennium*. Georgetown Public Law Research Paper No. 2. Baden-Baden: F.R.G.
 <<http://ssrn.com/abstract=1401357>>

Cita recomendada

DE TERWANGNE, Cécile (2012). «Privacidad en Internet y el derecho a ser olvidado/derecho al olvido». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 13, pág. 53-66. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_esp>

ISSN 1699-8154



Los textos publicados en esta revista están -si no se indica lo contrario- bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Acerca de la autora

Cécile de Terwangne

cecile.deterwangne@fundp.ac.be

La profesora Cécile de Terwangne tiene un máster en Derecho de la Universidad de Lovaina, un doctorado en Derecho de la Universidad de Namur y una licenciatura en Derecho Europeo e Internacional del Instituto Universitario Europeo de Florencia. Es catedrática de la Facultad de Derecho de la Universidad de Namur (Bélgica). Imparte clases de Ordenadores y derechos humanos, y Protección de datos. Es directora de investigación del CRIDS (Centro de Investigación sobre la Información, Derecho y Sociedad).

Université de Namur - Faculté de Droit

Rempart de la Vierge 5

B-5000 Namur, Bélgica

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet»

ARTÍCULO

El olvido: El derecho a ser diferente... de uno mismo Una reconsideración del derecho a ser olvidado

Norberto Nuno Gomes de Andrade

Fecha de presentación: noviembre de 2011

Fecha de aceptación: noviembre de 2011

Fecha de publicación: febrero de 2012

Resumen

Este artículo propone una nueva conceptualización del derecho a ser olvidado, argumentando a favor de su construcción teórica y aplicación concreta amparadas en el derecho a la identidad. Desde esta perspectiva, el artículo pretende arrojar una nueva luz sobre el derecho a ser olvidado contribuyendo a una conceptualización y una exigibilidad más desarrolladas al tiempo que aclara su ámbito de aplicación.

Basándose en la distinción entre el derecho a la identidad y el derecho a la privacidad, el artículo presenta las ventajas de relacionar el derecho a ser olvidado con el derecho a la identidad. Con esa conceptualización basada en el derecho a la identidad, se afirma que el derecho a ser olvidado también debe aplicarse al contenido generado por los usuarios y la información tratada para fines personales eliminando la exención para actividades domésticas establecida en la directiva europea sobre protección de datos. El artículo también sostiene que el derecho al olvido, enmarcado como parte del derecho a la identidad personal, también debe abordar hechos públicos e información, ofreciendo una justificación racional y más fuerte con la que alcanzar un equilibrio mejor y más justo con el derecho a la libertad de información con el que compete.

En el artículo se comentan los conflictos de derechos más relevantes que el derecho a ser olvidado tendrá que abordar, es decir, el conflicto con la libertad de expresión y el conflicto con la necesidad de preservar la memoria social.

Como ramificación del derecho a la identidad, el derecho a ser olvidado se presenta como el derecho a ser diferente, no de los demás sino de uno mismo, es decir, de lo que uno era antes. El derecho a ser olvidado también subraya el proceso de creación de identidad no solo constructivo, sino también deconstructivo.

Palabras clave

derecho a ser olvidado, derecho a la identidad personal, privacidad, protección de datos

Tema

Ley sobre tecnologías informáticas, Ley de protección de datos

Oblivion: The Right to Be Different ... from Oneself Reproposing the Right to Be Forgotten

Abstract

This article proposes a new conceptualization of the right to be forgotten, arguing in favour of its theoretical construction and concrete application under the umbrella of the right to identity. Following this perspective, I intend to shed new light on the right to be forgotten, contributing to a more developed conceptualization and enforceability while clarifying its scope of application.

Based on the distinction between the right to identity and that of privacy, the paper presents the advantages of associating the right to be forgotten with the right to identity. Through this identity-oriented conceptualization, I claim that the right to be forgotten should also be applied to user-generated content and information processed for personal purposes, overriding the 'household exemption' established in the European Data Protection Directive. I also argue that the right to oblivion, framed as part of the right to personal identity, should address public facts and information, providing a stronger rationale and justification to attain a better and fairer balance with the competing right to freedom of information.

The article then comments on the most relevant conflicts that the right to be forgotten will have to address vis-à-vis the freedom of expression and the need to preserve social memory.

As a branch of the right to identity, the right to be forgotten is presented as the right to be different, not from others but from oneself, i.e. from the one(s) we were before. The right to be forgotten also underlines the process of identity creation as not only constructive but also de-constructive.

Keywords

right to be forgotten, right to personal identity, privacy, data protection

Topic

IT Law, Data Protection Law

1. Introducción

1.1. El resurgimiento del debate y la convergencia hacia la adopción de un derecho a ser olvidado

El derecho a ser olvidado, también conocido como el derecho al olvido, *droit à l'oubli* (en francés) o *diritto all'oblio* (en italiano), es un instrumento jurídico complejo

e intrigante. El debate sobre este derecho, definido como «el derecho a silenciar acontecimientos pasados de la vida que ya no ocurren»,¹ se ha retomado recientemente en Europa. Debido a los sobresalientes desarrollos de las TIC, es decir, la digitalización y la proliferación de la información,² y su almacenamiento por defecto, se ha planteado inexorablemente la cuestión de la necesidad, oportunidad y viabilidad de un instrumento jurídico específico y más amplio para eliminar información.

1. Pino, 2000, pág. 237.

El tema del derecho a ser olvidado plantea la cuestión de conceder (o no) a los usuarios de Internet la posibilidad de suprimir los datos personales (como imágenes, textos, opiniones, documentos oficiales, certificados y cualquier otro tipo de datos personales que describen los comportamientos y acciones pasadas) de la lista de resultados servida por los motores de búsqueda o publicados en sitios web, redes sociales, blogs, etc. De hecho, esa cuestión -muy centrada en el derecho a ser olvidado- se ha explorado en debates políticos,³ encuestas,⁴ casos judiciales,⁵ propuestas legislativas,⁶ escritos académicos⁷ e iniciativas tecnológicas.⁸

Hay, pues, una convergencia generalizada y consensuada al parecer hacia la adopción y la consagración de un dere-

cho a ser olvidado. Sin embargo, centrándose concretamente en el aspecto legal, se ha hecho poco esfuerzo en la teorización del derecho a ser olvidado. El ejercicio que me propongo desarrollar en la siguiente sección es examinar el derecho a ser olvidado de una forma ligeramente diferente a la que generalmente se sigue. Así que voy a ir más allá de la caracterización del derecho al olvido como una simple etiqueta o dimensión del derecho a la privacidad. En este sentido, voy a reconstruir el retrato del árbol genealógico del derecho a ser olvidado, vinculándolo no al derecho a la privacidad o la protección de datos, sino al derecho a la identidad. Para ello, voy a necesitar, en primer lugar, distinguir y articular claramente estos tres derechos diferentes.⁹

2. La humanidad nunca antes ha producido, almacenado e intercambiado una cantidad tan impresionante de información. Con más de 1.970 millones de usuarios de Internet en todo el mundo, hoy en día, cada mes se comparten un promedio de 30 mil millones de artículos de contenido (enlaces, noticias, blogs, notas, álbumes de fotos, etc.) en Facebook, se crean 235 nuevos sitios web cada 90 segundos, se publican en Twitter más de 119 millones de mensajes todos los días, se cargan 35 horas de videos en YouTube cada minuto, y 1,2 millones de editores publican 11 millones de artículos al mes (<http://www.onlineschools.org/state-of-the-internet/soti.html>).
3. El derecho al olvido se ha propuesto recientemente como un derecho explícito que debe consagrarse en legislación específica. Para ello, tanto en Francia como en Italia se han presentado propuestas legislativas en este sentido. En Francia, además, se ha adoptado un código de buenas prácticas sobre el derecho a ser olvidado en las redes sociales y motores de búsqueda (*Charte du droit à l'oubli numérique dans les sites collaboratifs moteurs et de recherche*), de subscripción voluntaria. En la UE, la Comisión Europea (CE) ha propuesto la promulgación de un derecho específico a ser olvidado dentro de su proyecto de revisión del marco legal de protección de datos. Como se indica en la comunicación *Un enfoque integral sobre protección de datos personales en la Unión Europea*, la CE «examinará las formas de aclarar el llamado derecho a ser olvidado, es decir, el derecho de las personas a que sus datos no se traten y se eliminen cuando ya no sean necesarios para fines legítimos» (CE, 2010, pág. 8). El Supervisor Europeo de Protección de Datos (SEPD), en este sentido, ha ido más allá, proponiendo la codificación del derecho al olvido (SEPD, 2011, pág. 19).
4. Según los resultados de una encuesta muy reciente sobre las actitudes de los ciudadanos de la UE y los comportamientos en materia de gestión de identidad, protección de datos y privacidad, una clara mayoría de los europeos (75%) apoya el derecho a ser olvidado. Como se indica en el informe, quieren ser capaces de borrar la información personal en un sitio web cada vez que deciden hacerlo (CE, 2011).
5. El derecho a ser olvidado también se ha invocado en litigios y casos judiciales. Un caso reciente es el de la Agencia Española de Protección de Datos (AEPD) que ordenó a Google que retirara de sus listas de búsqueda casi 100 enlaces a sitios web que contenían información caduca o inexacta sobre ciertas personas, alegando el incumplimiento del derecho a la privacidad de los sujetos y, sobre todo, de su derecho a ser olvidados.
6. Véase la reciente propuesta de la Comisión Europea de un Reglamento general de protección de datos (CE, 2012), en particular el artículo 17 «Derecho al olvido y a la supresión».
7. Algunos académicos también han presentado sugerencias originales que forman modalidades interesantes de un derecho al olvido. Este es el caso de la idea de la *quiebra de la reputación* de Zittrain. Según el profesor de Harvard, a la gente se le permitiría declarar una quiebra de reputación cada diez años aproximadamente, dejando su reputación en blanco (eliminando ciertas categorías de calificaciones u otra información sensible) y empezar de nuevo (Zittrain, 2008, pág. 229). También se han presentado propuestas innovadoras para hacer cumplir un verdadero derecho a ser olvidado. Este es el caso de Mayer-Schönberger, quien en su libro *Delete: the virtue of forgetting in the digital age* (2009), sostiene que la tecnología digital y las redes globales están erosionando nuestra capacidad natural para olvidar y propone establecer fechas de caducidad de la información.
8. Varios investigadores de la Universidad de Washington han desarrollado una tecnología llamada Vanish que hace que los datos electrónicos se autodestruyan tras un período determinado (Rosen, 2010). Entre las muchas herramientas que permiten a los usuarios extraer datos de los sitios sociales, también se puede mencionar la empresa alemana de nueva creación X-Pire, que lanzó un programa de software que permite a los usuarios adjuntar fechas de caducidad digitales a las imágenes cargadas en sitios como Facebook (<http://www.x-pire.de/index.php?id=6&L=2>).
9. Para una explicación mas detallada sobre la diferencia entre los derechos de protección de datos, privacidad e identidad y su articulación, véase Andrade 2011.

2. Protección de datos - Privacidad - Identidad

Para entender el derecho al olvido, primero tenemos que situarlo en el marco jurídico vigente. Dado que el reciente debate sobre la adopción de un derecho general a ser olvidado se refiere a la cuestión de si los usuarios de Internet deberían tener derecho o no a borrar la información personal que circula en Internet, el lugar natural para volver a conceptualizar el derecho a ser olvidado parece ser el marco legal que regula el tratamiento de los datos personales, es decir, la legislación sobre protección de datos.¹⁰

El siguiente paso es analizar el conjunto más amplio de los derechos en virtud de los cuales el derecho a ser olvidado opera dentro de la legislación sobre protección de datos. Aquí nos encontramos no solo el derecho a la protección de datos, sino también el derecho a la privacidad y el derecho a la identidad. Es importante distinguir estos tres derechos para comprender mejor el derecho al olvido y para sustentar su conceptualización en el marco del derecho a la identidad. Por lo tanto, en primer lugar, y en términos muy sintéticos, distinguiré la protección de datos de la privacidad y la identidad. Luego, haré la distinción entre el derecho a la privacidad y el derecho a la identidad.

2.1. Protección de datos frente a privacidad/ identidad

Para entender las diferencias subyacentes en el alcance, la naturaleza y la razón de ser entre estos tres derechos, es importante reconocer y calificar el derecho a la protección de datos como un derecho procesal, mientras que el derecho a la privacidad y el derecho a la identidad son derechos sustantivos.

Los derechos sustantivos se crean para garantizar la protección y promoción de los intereses que el individuo humano y

la sociedad considera que es importante defender y preservar. Los derechos procesales funcionan a un nivel diferente, establecen reglas, métodos y condiciones para que los derechos sustantivos se apliquen y protejan eficazmente. La protección de datos, como tal, no representa directamente un valor o interés *per se*, prescribe los procedimientos y métodos para lograr el respeto de los valores encarnados en otros derechos -como el derecho a la privacidad, a la identidad, a la libertad de información, a la seguridad o a la libertad de religión. Los requisitos de procedimiento, como los relativos a la transparencia, la accesibilidad y la proporcionalidad, funcionan como condiciones indispensables para la articulación y coordinación entre diferentes intereses y derechos.¹¹ Por tanto, es erróneo reducir la protección de datos a la privacidad,¹² ya que la primera protege un conjunto mucho más amplio de intereses y derechos. Según este marco, el derecho a ser olvidado es un derecho de protección de datos, ya que establece un procedimiento específico (la posibilidad de solicitar la eliminación de la información) con el fin de lograr la protección de un interés y derecho sustantivo determinado. La pregunta que surge es definir ¿qué interés protege el derecho a ser olvidado: privacidad o identidad?

2.2. Privacidad frente a identidad

El derecho a la privacidad y el derecho a la identidad comparten el mismo ADN. Ambos forman parte de un conjunto más amplio de derechos llamados derechos de la personalidad y, como tales, ambos derivan de los derechos fundamentales a la dignidad y la autodeterminación. Sin embargo, hay diferencias importantes entre estos dos derechos.

El derecho a la identidad se puede definir, de una manera muy básica, como el derecho a que las señas, los atributos o las facetas de la personalidad que son características de una persona en particular (como la apariencia, el nombre, el carácter, la voz o la historia de su vida) sean reconocidos

10. Como hemos visto en la reciente propuesta de la Comisión Europea, es en el ámbito de esa legislación que se considera la posibilidad concreta de borrar los datos personales propios.
11. La aplicación de la directiva de protección de datos es un excelente ejemplo de un ejercicio de procedimiento de este tipo. Para conciliar el derecho a la intimidad con el libre intercambio de información, en el mercado interior, la directiva establece una serie de directrices y principios de procedimiento para lograr ese equilibrio (los principios básicos que se resumen en el artículo 6 de la directiva de protección de datos).
12. En efecto, la Carta de los Derechos Fundamentales de la Unión Europea (que, con la entrada en vigor del Tratado de Lisboa, adquirió efecto jurídico vinculante en igualdad con los Tratados) ya establece la protección de datos como un derecho independiente y autónomo (artículo 8) distinto del derecho a la privacidad (consagrado en el artículo 7).

y respetados por los demás. La jurisprudencia italiana añadió una dimensión más sustantiva al derecho a la identidad personal y lo describió como «el derecho que todo el mundo tiene a comparecer y ser representado en la vida social (en especial por los medios de comunicación) de una manera que se corresponda, o que por lo menos no falsee o distorsione, su identidad personal».¹³ Según esta afirmación, el derecho a la identidad personal se refiere a la imagen correcta que uno quiere proyectar en la sociedad. A un nivel más general, el derecho a la identidad puede definirse como el «derecho a ser uno mismo»,¹⁴ es decir, el derecho a ser diferente de los demás, el derecho a ser único. Como ha observado Neethling, el derecho a la identidad de una persona refleja el «interés definitivo e inalienable en la singularidad de su ser».¹⁵ Según esta conceptualización, la identidad de una persona se vulnera si cualquiera de sus señas se usan sin autorización de modos que no puedan conciliarse con la identidad (y la imagen o proyección social) que quería transmitir.

Después de haber dicho en otro lugar que la definición excesivamente amplia del derecho a la privacidad, seguido por la doctrina dominante en este campo, ha socavado y pasa por alto el concepto y el derecho a la identidad, entiendo el derecho a la privacidad en términos más delimitados de los que generalmente se establecen. El derecho a la privacidad protege un interés que se ha definido como «una condición personal de vida que se caracteriza por la reclusión del público y, por lo tanto, carencia de conocimiento por el público».¹⁶ En estos términos, la privacidad solo se puede vulnerar mediante el conocimiento no autorizado de terceras personas de hechos y asuntos privados.

Para recapitular, la privacidad -vista desde una perspectiva más clásica y delimitada como un derecho a la opacidad o al aislamiento- se refiere principalmente a la ocultación de algunos aspectos particulares del conocimiento público y la protección de la información divulgada de la esfera pública. La identidad, en cambio, se refiere a la transmisión de información a la esfera pública, es decir, a su correcta expresión y representación a ojos del público. Además, según esta distinción, cada derecho

se vulnera y viola de manera diferente. El derecho a la identidad se vulnera si la persona A hace uso de las señas de identidad (atributos) de la persona B de una manera contraria a la forma en que la persona B percibe su identidad (cuando la identidad de la persona B se falsifica o cuando se transmite una imagen errónea de su personalidad). El derecho a la privacidad, en cambio, solo se vulnera si se revelan al público hechos privados relacionados con una persona.

Esta distinción es de vital importancia para la conceptualización del derecho a ser olvidado amparándolo en el derecho a la identidad. Como veremos en la siguiente sección, argumento que el derecho al olvido se debe entender como un derecho de protección de datos (un derecho de procedimiento) que principalmente persigue y protege un interés de identidad (un derecho sustantivo) que se propone hacer cumplir el derecho de un individuo a la identidad personal.

3. El derecho a ser olvidado: una perspectiva de identidad

El derecho a ser olvidado, como el derecho de los individuos a hacer que se elimine información sobre ellos después de un cierto período de tiempo, no solo atañe a un interés fundamental de la identidad, sino que también desarrolla y enriquece la conceptualización del derecho a la identidad personal. El derecho al olvido subraya no solo el derecho a ser diferente de los demás, sino también el derecho a ser diferente de uno mismo, es decir, de uno mismo en el pasado. Este es un matiz muy importante, ya que llama la atención sobre el papel esencial que desempeña el derecho a ser olvidado para permitir la deconstrucción de la identidad antes de poder construir una identidad nueva y diferente.

Partiendo de la afirmación fundamental de que el derecho al olvido debe estar anclado en el derecho a la identidad, en esta sección se describen las principales ventajas que ofrece esta reconceptualización.

13. Pino, 2000, pág. 225.

14. Esta expresión corresponde a la definición dada al derecho a la identidad por el Tribunal Constitucional italiano, *diritto ad essere sé stesso* (3.2.1994, n.13). Para un análisis más profundo, véase Pino, 2003 y Trucco, 2004.

15. J. Neethling, Potgieter y Visser, 1996, pág. 39.

16. Johann Neethling, 2005, pág. 233.

3.1. Ámbito de aplicación más amplio

3.1.1. Hechos públicos

Como mucha de la información que los individuos desean eliminar ya está en el registro público (siendo esa precisamente la razón de que la quieran eliminar), se han planteado objeciones con respecto a la calificación del derecho a ser olvidado como un derecho a la privacidad. En este sentido y como Gutwirth ha observado, «[...] es muy dudoso que ese *derecho a ser olvidado* pueda interpretarse como una ramificación del derecho a la privacidad, ya que la mayoría de los conflictos de tiempo conciernen a hechos públicos (por ejemplo, las personas involucradas como víctimas o como testigos de un crimen) que no están protegidas por el derecho a la privacidad».¹⁷ El argumento básicamente dice que, dado que los derechos de privacidad solo se ocupan de la información privada, no pueden abordar la información pública y tratarla como privada. Esta objeción implica cuestiones de libertad de expresión (en concreto, de libertad de prensa), ya que generalmente se considera que la prensa puede divulgar la información que forme parte de un registro público.¹⁸

Teniendo en cuenta que el derecho a la privacidad trata de proteger que la información privada se divulgue a la esfera pública, mientras que el derecho a la identidad atañe a la transmisión de información a la esfera pública, concretamente a su proyección y representación correcta ante el público, el derecho a ser olvidado solo puede referirse a la información que ya es de dominio público (hechos públicos) si se considera como una ramificación del derecho a la identidad y no del derecho a la privacidad. En otras palabras, la introducción de un derecho al olvido relacionado con el derecho a la identidad personal soluciona el problema identificado anteriormente, lo que le permite abordar también los hechos y la información que ya han sido divulgados al público. El objetivo del derecho al olvido, en muchos casos, no es ocultar información privada del conocimiento público, sino eliminar información pública y así evitar una divulgación más amplia.

3.1.2. La información descontextualizada

Recapitulando la distinción entre el derecho a la privacidad y a la identidad presentados anteriormente, se debe tener en cuenta que el derecho a la identidad atañe a todos los datos personales –sin importar si son ciertos o no– que puedan falsificar o transmitir una imagen errónea de la propia identidad. El derecho a la privacidad, en cambio, comprende solo los hechos personales que forman parte de la esfera privada y que no son (o no deberían ser) de dominio público. Como Pino añade, es posible «distinguir el derecho a la identidad personal tanto de la reputación como de la privacidad. En el primer caso, en efecto, cabe señalar que las declaraciones falsas no tienen que ser necesariamente difamatorias: la identidad personal puede ser violada también por la atribución de (falsos) méritos. En el caso de la privacidad, en cambio, la protección legal no se refiere a la exposición correcta de la personalidad a los ojos del público, sino más bien el interés del interesado de no ser expuesto».¹⁹ Respecto a esto último, me gustaría añadir y especificar que el derecho a la privacidad solo protege el interés del individuo de ocultar hechos o aspectos ciertos del conocimiento público.

Una vez aclarado el espacio conceptual y el tipo de información protegida por el derecho a la privacidad y a protegerse de la difamación, seguimos con un tipo específico de información que no está regulada por ninguno de estos derechos: la información descontextualizada, es decir, falsa en última instancia (pero no calumnias o difamaciones) o no necesariamente veraz. Este es exactamente el tipo de información que atañe al derecho a ser olvidado desde una perspectiva de identidad, es decir, la información que con el paso del tiempo queda descontextualizada, distorsionada, anticuada, que ya no es verdad (pero no necesariamente falsa) y que ofrece al público una representación errónea de la identidad del individuo.

En resumen, la asociación del derecho a la identidad personal con el derecho a ser olvidado permite a este último hacer frente a ciertas categorías de información que su conceptualización como un derecho a la privacidad no le permitirían cubrir. Es el caso de la información pública y descontextualizada (ya no verdadera). En otras palabras,

17. Gutwirth, 2009.

18. En este sentido, véanse las sentencias del Tribunal Supremo de Estados Unidos en *Cox Broadcasting Corp. v. Cohn* (1975) y *Florida Star v. B.J.F.* (1989), que afirman que los periodistas tienen derecho a publicar la información pública.

19. Pino, 2000.

el derecho a ser olvidado, como parte del derecho a la identidad, interviene en los espacios no cubiertos por la protección contra la difamación y el derecho a la privacidad, abarcando la información que, o bien pertenece ya al dominio público o que ya no es verdad (pero no necesariamente constituye difamación) dado el paso del tiempo y la ocurrencia de otros acontecimientos. El derecho a la identidad personal, de esta manera, mejora la admisibilidad y la aplicación del derecho a ser olvidado, ampliando su ámbito de aplicación.

3.1.3. La exención de las actividades domésticas y la prevalencia infalible del derecho a la libertad de expresión

Por regla general, la directiva de protección de datos se puede aplicar siempre que haya tratamiento de datos personales (es decir, datos relativos a una persona física identificada o identificable). Sin embargo, se contemplan exenciones y la directiva no se aplica, por ejemplo, a las personas que tratan datos personales «en el ejercicio de actividades exclusivamente personales o domésticas». En otras palabras, los principios y normas de protección de datos no se aplican a las personas que usan datos personales solo para sus propios fines domésticos y recreativos.

Dada la confusión cada vez mayor entre los lugares, actividades o fines públicos y privados permitidos por el desarrollo de las TIC, lo que la directiva de protección de datos entendía por «actividades exclusivamente personales» en el año 1995 es hoy muy cuestionable. Con el establecimiento de la exención para actividades domésticas, a mediados de los noventa, la directiva de protección de datos partía de la suposición de que los datos personales tratados para fines domésticos no planteaban riesgos de privacidad o problemas de responsabilidad por parte de los responsables del tratamiento, ya que solo tratarían esos datos para sus pro-

prios fines privados. La directiva también suponía que el tratamiento de los datos para fines personales implicaría un círculo restringido de personas íntimas y, por tanto, no implicaría la expectativa o la necesidad de proteger la privacidad de los individuos identificados por esos datos. Sin embargo, la aparición y consolidación de las redes sociales están poniendo en cuestión estas hipótesis. De hecho, estos supuestos están en desacuerdo con la realidad actual. La publicación de información personal en redes sociales, incluso si se hace por razones puramente personales o recreativas, implica muchas veces la divulgación de información a grandes audiencias.²⁰ Y esto invalida la hipótesis de que los datos solo circulan dentro de un círculo restringido de personas íntimas y que su divulgación no presenta riesgos para la privacidad.²¹ Hay una necesidad urgente de aclarar las reglas aplicables al tratamiento de datos por particulares con fines privados y, además, su articulación con otra regla de excepción de la protección de datos, concretamente, el tratamiento de datos realizado exclusivamente con fines periodísticos y protegido por el derecho a la libertad de expresión (el artículo 9 de la Directiva de protección de datos). ¿Qué se debe entender por «actividades exclusivamente personales»? ¿La publicación de la información en una red social equivale a la divulgación de información para fines privados, es decir, a nuestro grupo privado (probablemente grande) de contactos seleccionados? ¿O es equiparable a la divulgación de información al público?²² Si es así, hay otra perspectiva que hay que tener en cuenta. Los particulares que divulgan información, opiniones o ideas al público -por ejemplo, en redes sociales, blogs, Youtube o Twitter- estarían entonces protegidos por la libertad de expresión y recibirían el mismo trato que los profesionales de los medios de comunicación que tratan datos «con fines exclusivamente periodísticos o de expresión artística o literaria». En consecuencia, estarían exentos de ciertas disposiciones de la legislación sobre protección de datos si fuese necesario conciliar el derecho a la protección de datos con las normas que rigen la libertad de expresión. Esto significa

20. El usuario promedio de Facebook tiene 130 amigos y está conectado a 80 páginas, grupos y eventos de la red social (<http://www.facebook.com/press/info.php?statistics>).

21. El Grupo de Trabajo sobre Protección de Datos del Artículo 29, en este sentido, ha aclarado varios casos en los que la actividad de una red social puede no quedar exenta por la excepción para actividades domésticas, concretamente «cuando la red social se utiliza como una plataforma de colaboración para una asociación o una empresa» o «cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen a la red social pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda». Como señala en su dictamen, «un gran número de contactos puede indicar que no se aplica la excepción doméstica y el usuario podría entonces ser considerado como un responsable del tratamiento de datos» (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2009, pág. 6).

22. Entonces surge una cuestión adicional: Según cuantas personas tengan acceso a esa información ¿su difusión se consideraría como tratamiento de datos personales con fines privados o como divulgación al público?

que a la mayor parte de la información divulgada en Internet y susceptible de ser eliminada (fotos en redes sociales, comentarios en blogs, vídeos en Youtube) no se le aplicarían las normas de protección de datos (ya sea como datos tratados para fines personales o protegidos por la libertad de expresión) y, por tanto, no quedaría protegida por el derecho a ser olvidado.²³

Para evitar la aplicación de la exención de las actividades domésticas²⁴ o la salvaguarda de la libertad de expresión al derecho a ser olvidado, este derecho se debe relacionar con el derecho a la identidad. Esto permitiría la posibilidad de solicitar la eliminación de información personal publicada en Internet, tanto la tratada para fines exclusivamente personales (y que no se divulga más allá del número de contactos elegidos) como la publicada para el público general y accesible a un número indefinido de personas. En cuanto a la información divulgada al público, el derecho al olvido enmarcado en el derecho a la identidad presenta una justificación más fuerte en el proceso de equilibrio con el derecho a la libertad de expresión, evitando así la prevalencia infalible de esta última. Los criterios para la aplicación del derecho a ser olvidado se referirían a la ocurrencia de una representación errónea de la identidad propia, es decir, la verificación de un desajuste entre la identidad que transmite la información obsoleta y la que el individuo desea transmitir en ese momento. En resumen, el derecho al olvido podría aplicarse sin tener en cuenta si la información en cuestión se hubiera publicado para el ejercicio de actividades domésticas o no y sin tener en cuenta si la información se hiciera accesible a un número indeterminado de personas o no. Este cambio paradigmático desde un argumento de privacidad a uno de identidad haría la exención para actividades domésticas (y todas las complejidades actuales en torno a tal disposición)²⁵ inaplicable al derecho a ser olvidado. También dotaría al derecho al olvido de una justificación más fuerte para el

equilibrio y la articulación con el derecho a la libertad de expresión cuestionando su prevalencia infalible. Con esta nueva conceptualización (basada en el derecho a la identidad), el derecho a ser olvidado vería su ámbito de aplicación considerablemente ampliado.

3.2. La identidad como la raíz normativa del derecho al olvido

La conceptualización propuesta del derecho a ser olvidado no solo tiene sentido desde un punto de vista de la identidad, sino que también contribuye a un mayor desarrollo de la concepción moderna de la identidad, reforzando su comprensión «antiesencialista».²⁶

Siguiendo a Pino en este asunto, la identidad personal no debe ser caracterizada como inmutable y contingente, algo que se tiene *per natura*. La identidad es más bien una construcción cultural y social, algo que elegimos, construimos y respetamos.²⁷ La identidad personal se debe percibir como una cuestión de opciones, un proceso de negociación continua (con nosotros mismos y con los demás), no predeterminada y unívoca, sino que se puede revisar y cambiar constantemente. El derecho a ser olvidado se erige como un importante instrumento para ser usado en el proceso de negociación, ampliando más opciones, permitiendo identidades futuras mediante la eliminación de las anteriores.

Se pueden encontrar ideas similares en la conceptualización de la identidad personal como una narrativa²⁸ según la cual las identidades personales se conciben y se entienden mejor como historias (que nos contamos a nosotros mismos y a los demás). Según esa conceptualización, las identidades no solo son nómadas, cambiando según el

23. Sin embargo, es importante tener en cuenta que estas posibles exenciones de las leyes de protección de datos no excluyen la posibilidad de que los titulares de los datos personales puedan usar recursos civiles y penales desarrollados bajo la legislación nacional para hacer efectivo su derecho a la vida privada (contra bloggers privados, usuarios de Twitter, etc.).

24. Sin embargo, y como el Grupo de Trabajo sobre Protección de Datos del Artículo 29 observó: «cabe señalar que, aunque se aplique la exención doméstica, un usuario puede ser responsable en virtud de las disposiciones generales del derecho civil o penal nacional en cuestión (en particular, difamación, responsabilidad por violación del derecho a la personalidad o responsabilidad penal)» (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2009, pág. 7).

25. Para una explicación detallada de la situación en la que las actividades de un usuario de una red social están cubiertas por la exención para actividades domésticas o no, véase Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2009.

26. Pino, 2010, pág. 297.

27. Pino, 2010, pág. 297.

28. Ricoeur, 1992.

movimiento de la historia, sino que también permanecerán abiertas a la revisión. Teniendo en cuenta la idea de la identidad personal como una narrativa, y ampliándola un poco más, la cuestión que subyace al derecho al olvido es la posibilidad de hacer que las partes de nuestra identidad narrativa se borren, evitando que sean accesibles y reconocidas por el público en general. En este sentido, el derecho a ser olvidado amplía el alcance del derecho a la identidad personal, abarcando no solo el derecho a construir la futura historia de nuestra identidad, sino también el derecho a borrar nuestro pasado. El derecho a ser olvidado, de esta manera, juega un papel esencial no en el proceso de construcción de la identidad, sino en el proceso de deconstrucción de la identidad, permitiendo construir después identidades nuevas y diferentes.

La conceptualización del derecho al olvido desde la perspectiva de la identidad, por otra parte, sigue la línea *antisencialista* mediante la cual la ley ha estado regulando la identidad personal. De hecho, la ley ha dotado a los individuos con más y más instrumentos legales con los que pueden influir y cambiar aspectos de su identidad. Las personas, hoy en día, tienen derecho a romper las cadenas de filiaciones, modificar nombres, abandonar nacionalidades y cambiar de sexo.²⁹ El derecho a eliminar parte de nuestra identidad parece encajar muy bien en esta forma de entender y tratar la identidad personal que la ley apoya desde hace tiempo.

En esta propuesta de conceptualización, se debe tener en cuenta que, al contrario de otros derechos de la personalidad, la identidad personal cambia con la evolución y el envejecimiento de la persona.³⁰ Añadiendo a esta particularidad una de las principales justificaciones del derecho a la identidad personal -el derecho a que no se falsee o malinterprete nuestra identidad, parece que los caracteres variables y cambiantes de la identidad personal exigen el derecho a que

los demás reconozcan y confirmen nuestra identidad más reciente y actual.³¹ Esto implica, a su vez, el derecho a hacer que se eliminen los rastros anteriores de la propia identidad (tanto si van en contra de nuestra identidad real y actual como si no), es decir, hacer que se borren los datos y las acciones representativas de identidades pasadas (si así lo deseamos). Ya que solo olvidando las identidades pasadas podemos hacer que prevalezca la identidad real, el derecho a ser olvidado puede desarrollar un papel muy importante para que una persona pueda reconstruir su narrativa identitaria, teniendo la certeza de que las identidades pasadas no ponen en peligro ese proceso.

En este sentido, el derecho al olvido parece encontrar una raíz normativa adecuada en el derecho a la identidad personal. De hecho, el derecho a ser olvidado está en el núcleo del interés y valor principales que trata de lograr el derecho a la identidad personal: el interés por la propia singularidad, el interés por ser diferente de los demás y de uno mismo, es decir, del que uno era antes. En consecuencia, el derecho al olvido -como parte del derecho a la identidad personal- está íntimamente ligado a la capacidad de reinventarse, de tener una segunda oportunidad, de empezar de nuevo y presentar una identidad renovada al mundo.

4. Conflictos y equilibrios

El control perfecto y completo sobre la propia proyección y construcción de la identidad no solo es indeseable, sino también imposible. Como constructo social, la identidad personal incluye la propia autopercepción (*ipse*, cómo una persona se percibe a sí misma), así como la percepción que otros tienen de nosotros mismos (*idem*, cómo nos perciben y representan los otros).³² En otras palabras, nuestra identidad personal está también (e inexorablemente) construida

29. Pousson, 2002, pág. 529; De Hert, 2008, pág. 12.

30. Niger, 2008b, pág. 125.

31. Continuando con este punto de vista, Niger observa que la necesidad de proteger la propia proyección en la realidad de la sociedad, teniendo en cuenta lo que uno es y expresa mediante su presencia social actual, tiene una importancia enorme. El pasado de una persona, siempre y cuando no sea necesario para definir la propia presencia social real y actual, debería permanecer en el olvido, concretamente, cuando su recuerdo puede alterar su posición actual. (Niger, 2008a - traducción del autor)

32. Esta distinción equivale a la diferencia entre la identidad *ipse* e *idem*: «[i]dem (el mismo) se refiere a la tercera persona, la perspectiva de observación objetiva de la identidad como un conjunto de atributos que permite la comparación entre las personas, así como una única identificación, mientras que *ipse* (uno mismo) representa la perspectiva en primera persona que constituye un *sentido de uno mismo*. Su intersección permite la construcción de la identidad de una persona» (M. Hildebrandt, 2009, pág. 274). Véase también Mireille Hildebrandt, 2006. Paul Ricoeur (1992) fue el primero en proponer esta distinción en filosofía.

por terceras personas, está conformada por las percepciones que *otros* tienen de nosotros. Hay, pues, un diálogo inevitable entre el individuo y los otros en el proceso de construcción de identidad personal. Esto significa que las peticiones de supresión de información relativa a la identidad personal también deben tener en cuenta los intereses que los demás (como colectividad) pueden tener en el mantenimiento de dicha información y la correspondiente identidad de las huellas *vivas*.

A pesar de los argumentos presentados en favor del desarrollo de un derecho a ser olvidado, es sumamente importante tener en cuenta que el derecho al olvido no es un derecho absoluto. De hecho, el derecho a ser olvidado vive en permanente tensión y conflicto con otros derechos, intereses, valores y objetivos. Un ejemplo claro se puede encontrar en las leyes de protección de datos que prescriben la obligación de conservar los datos durante períodos de tiempo determinado. Impulsadas por motivos de seguridad pública (entre otros), esas leyes chocan con el derecho a ser olvidado. Entre los muchos otros ejemplos que podrían citarse, en esta sección se resumen dos de los principales conflictos que el derecho a ser olvidado tendrá que abordar.

4.1. El derecho a ser olvidado frente a la libertad de expresión/información

El interés (privado) y el derecho a ser olvidado tiene que equilibrarse y articularse con otros de los derechos e intereses en conflicto. Este es el caso del interés público y social a acceder a la información (derecho a la información), y del derecho a la libertad de expresión³³ (el derecho de la prensa a informar, que también incluye el derecho de las personas a ser informadas).

La propuesta de la Comisión Europea de establecer el derecho al olvido en la próxima revisión del marco legal de la protección de datos ha generado reacciones negativas, concretamente, en los Estados Unidos, donde la libertad de expresión se defiende y apoya con firmeza.³⁴ Estas objeciones son un resurgimiento del conflicto clásico entre la privacidad y la libertad de información. Los que sostienen el derecho a la información y la libertad de expresión en detrimento del derecho al olvido argumentan que el derecho de eliminar información sobre uno mismo equivale a un derecho a impedir que la gente hable acerca de una persona. Mayes, argumentando en contra del derecho a ser olvidado, ha comentado lo siguiente: «el olvido puede sonar atractivo para algunos, pero convertirlo en derecho degrada el concepto de derechos. En lugar de ser algo que encarna la relación entre el individuo y la sociedad, pretende que la relación no existe. El derecho a ser olvidado... es un producto de nuestra imaginación».³⁵

En contra de esta opinión, creo que es importante reconocer que el derecho al olvido abarca mucho más que la mera intención de ocultar al individuo de la sociedad (perspectiva de la privacidad). El derecho a ser olvidado es un instrumento mediante el cual los individuos corrigen y vuelven a proyectar sus imágenes a la sociedad (perspectiva de la identidad). Es en estos términos, como el derecho a transmitir la propia imagen e identidad que uno desea a la opinión pública, que el derecho al olvido se debe equilibrar y articular con el derecho a la libertad de información y la libertad de expresión. De esta manera, el derecho a ser olvidado no pasa por alto la relación entre el individuo y la sociedad. Por el contrario, el derecho a ser olvidado asume y parte de su existencia, reequilibrando de la forma en que se representa al individuo (y su identidad *ipse*) en la sociedad (identidad *idem*).

33. Véase el artículo 10 del Convenio Europeo de Derechos Humanos: «Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras».

34. Es interesante señalar que el derecho a ser olvidado no está protegido en los Estados Unidos, donde prevalecen el derecho a informar y el derecho a la libertad de expresión. Este hecho es consecuencia de la cada vez más amplia protección de la Primera Enmienda de la libertad de prensa y una clara preferencia por esta última sobre la privacidad de los individuos. Para más detalles sobre el enfrentamiento entre Europa y los Estados Unidos sobre la tensión entre el derecho a informar y el derecho a ser olvidado, véase Werro, 2009.

35. Mayes, 2011.

4.2. El derecho a ser olvidado frente al derecho a la memoria y la objetividad

Otro conflicto recurrente con el que se enfrentará el derecho al olvido atañe a la necesidad de preservar la memoria colectiva e histórica.³⁶ En este caso, el derecho a ser olvidado entra en conflicto con el interés histórico de mantener y archivar información de la actualidad. A diferencia de cualquier otro período en la historia, cada uno de nosotros crea un registro en línea de nuestras vidas, la compilación de nuestro legado digital personal. Como Paul-Choudhury señala, «todos estos datos resultarán fascinantes para los sociólogos, los arqueólogos y antropólogos que estudien los albores de la era digital. Para ellos, la vida cotidiana puede ser tan interesante como los momentos trascendentales que definen la época».³⁷

Este *argumento conservacionista*, sin embargo, parece ir de un extremo a otro, anunciando y celebrando el paso de un período en que la investigación histórica trataba de describir el pasado a partir de fuentes muy escasas a un período en el que la investigación histórica no deja abandonar el pasado, manteniéndolo vivo y actualizado preservando hasta el dato más nimio. La capacidad de eliminar parte de la propia identidad no se debe sacrificar, en la mayoría de los casos, en aras de este tipo de consultas *históricas*. De hecho, la investigación sobre un grupo particular (durante un período determinado) no siempre necesita el escrutinio de información personal, ya que los datos anónimos sirven para esos propósitos.

Otro argumento de los preservacionistas es el de la objetividad. En la disputa judicial entre la Agencia Española de Protección de Datos y Google, como se describió anteriormente, el motor de búsqueda se negó a eliminar los enlaces afirmando que estas acciones, si se hacen sistemáticamente, pondrían en peligro la objetividad de Internet y la transparencia de los motores de búsqueda. Los usuarios de Internet podrían eliminar información objetiva de Internet, manipulando así la lista de los resultados presentados por los motores de búsqueda, haciéndolos imprecisos e incompletos.

El derecho a ser olvidado como un intento de manipular algún tipo de objetividad de Internet o de memoria colectiva de la sociedad es un argumento poco convincente, cuando no infundado. En primer lugar, la idea de objetividad es bastante discutible, especialmente si procede de un motor de búsqueda que organiza sus listados de búsqueda mediante algoritmos enigmáticos y poco transparentes. En segundo lugar, negar el derecho individual a borrar la propia información personal que no tiene interés periodístico o relevancia histórica por mantener una supuesta memoria colectiva parece desequilibrado.³⁸ Ante esto, creo que hay un énfasis exagerado en un interés colectivo infundado en detrimento de un interés individual necesario, como el derecho a ser diferentes de lo que éramos antes.

4.3. Criterios para equilibrar derechos

Como he mencionado antes, el ejercicio del derecho al olvido puede chocar con otros derechos, generando conflictos con otros intereses protegidos que exigen un delicado equilibrio

36. Un ejemplo paradigmático de la preservación de una memoria colectiva relacionado con las nuevas tecnologías (en este caso en la denominada web 2.0) se refleja en el anuncio hecho por la Biblioteca del Congreso de Estados Unidos. La biblioteca más grande del mundo ha anunciado que va a archivar digitalmente todos los tweets públicos desde el inicio de Twitter en marzo de 2006 (Bean, 2010, consultado el 2 de octubre de 2010). Twitter es un sitio web que ofrece una red social y servicio de microblogging que permite a sus usuarios enviar y leer mensajes de otros usuarios llamados tweets (Wikipedia, <http://en.wikipedia.org/wiki/Twitter>) (consultado el 24 de julio de 2011).

37. Como el autor añade: «los recuerdos que ahora dejamos atrás, en toda su gloria desenfundada -tweets de borrachos, entradas de blog despotricando sobre esto y aquello, fotos de personas en días que se levantaron con el pie izquierdo y mucho más- pueden convertirse en un tesoro único para los estudios de los historiadores de los siglos futuros. De hecho, la web de hoy puede ofrecer la instantánea más veraz y completa de la raza humana que existe». (Paul-Choudhury, 2011). Para más información sobre la arqueología de Internet y cómo podría funcionar el olvido en línea, véase www.newscientist.com/special/digital-legacy.

38. Además, ya se ofrecen servicios que actúan directamente sobre la lista de resultados de búsqueda ofrecidos por los motores de búsqueda, manipulándolos o eliminándolos para pulir y reformar la propia imagen en Internet. Es el caso de la gestión de la reputación en línea: «la práctica de la vigilancia de la reputación de una persona en Internet, de una marca o empresa con el objetivo de suprimir totalmente menciones negativas o relegándolos a posiciones más bajas en la página de resultados de los motores de búsqueda para disminuir su visibilidad» (Wikipedia, http://en.wikipedia.org/wiki/Online_reputation_management) (consultado el 23 de julio de 2011).

de derechos. En este sentido, es importante observar que, de la misma manera que el derecho a ser olvidado no es una novedad, tampoco lo es el equilibrio de su aplicación con otros derechos e intereses. De hecho, la jurisprudencia ya ha desarrollado una serie de criterios importantes, que la legislación ha consagrado, para resolver algunos de estos conflictos. Es el caso del derecho penal, donde el derecho al olvido se desarrolló por primera vez. Efectivamente, en caso de conflicto entre el derecho al olvido del pasado judicial (a la supresión de la información sobre antecedentes penales y condenas pasadas) y el derecho a la información (acceso a dicha información), el factor tiempo se ha usado como un criterio decisivo. Si la información se considera de interés periodístico (debido a la actualidad de su ocurrencia), el derecho a la información prevalece; si no, el derecho al olvido prevalece sobre el derecho a la información (todavía se puede acceder a la sentencia, pero ya no se incluyen los nombres de los implicados).³⁹ Además, se prevén dos nuevas excepciones en las que el derecho a la información prevalece sobre el derecho al olvido. Estas atañen a hechos pertenecientes a la historia o considerados de importancia histórica, y hechos relacionados con las actividades de figuras públicas (cuyo comportamiento, debido a su papel y responsabilidad pública, ha de ser transparente para la sociedad).

Las leyes de protección de datos han formulado una serie de principios para el tratamiento lícito de datos personales, así como excepciones a su tratamiento legítimo, que también pueden ser usados para resolver algunos conflictos relacionados con el derecho a ser olvidado. El respeto por el principio de finalidad (según el cual se pueden tratar solo los datos relevantes para el propósito definido por su recogida) y el

respeto por el principio de proporcionalidad (que prohíbe el tratamiento de datos excesivos para una finalidad preestablecida) constituyen importantes criterios que, efectivamente, pueden contribuir a la resolución de casos conflictivos relacionados con el derecho al olvido. Además, la ley de protección de datos también establece excepciones y salvaguardas para el tratamiento de datos personales. Es el caso de las garantías adecuadas que los estados miembros tendrán que establecer para datos personales almacenados por largos períodos con fines históricos, estadísticos o científicos (Artículo 6 (e) de la directiva de protección de datos). Es también el caso, como ya he mencionado, de los datos recogidos exclusivamente con fines periodísticos o propósitos de expresión artística o literaria (artículo 9 de la directiva de protección de datos). Estas excepciones también se deben tener en cuenta al equilibrar el derecho al olvido con el derecho a la libertad de expresión.⁴⁰ Este proceso de equilibrio, además, debe tener en cuenta el interés periodístico de la información (como hemos aprendido de la jurisprudencia del derecho penal) y, añadido yo, la conceptualización del derecho a ser olvidado desde la perspectiva de la identidad. Este giro conceptual es importante, ya que puede mejorar la aplicabilidad del derecho a ser olvidado en detrimento de otros derechos (como hemos visto en el caso de la exención de las actividades domésticas, en las que el derecho al olvido no se aplicaría desde la perspectiva de la privacidad, sino desde la de la identidad).

Además, y en casos particulares, es importante reconocer que el derecho a ser olvidado no debe prevalecer siempre. Como Werro explica: «Cuando la información sobre el pasado es necesaria para proteger al público de hoy, no existirá derecho a ser olvidado. Por ejemplo, cuando una

39. En este caso, es importante señalar que el respeto por el principio de transparencia de la justicia no requiere la divulgación de los nombres y otros datos personales de las personas involucradas en las controversias judiciales. El propósito de este principio es permitir la transmisión de los conocimientos de la ley, permitiendo la argumentación jurídica que se desarrollará basándose en las decisiones y opiniones que ya existen.

40. Tal equilibrio se logra, efectivamente, en virtud de la ley italiana de protección de datos. Los periodistas pueden reunir, registrar y difundir los datos personales de un individuo sin su consentimiento solo si el tratamiento se lleva a cabo (1) en el ejercicio de la actividad periodística, (2) a los solos efectos relacionados con los mismos y (3) dentro de las limitaciones impuestas a la libertad de la prensa para proteger los derechos fundamentales de las personas y su dignidad, con especial referencia a la materialidad de la información con respecto a los hechos de interés público (véase el artículo 137 del Código de protección de datos italiano -Decreto legislativo n.º 196/2003- y el Código de conducta relativo al tratamiento de datos personales en el ejercicio de la actividad periodística, anexo A del Código de Protección de Datos).

El Tribunal Supremo italiano aclaró además los requisitos de cumplimiento que la prensa debe seguir para dar a conocer información personal legalmente: a) la verdad objetiva de la información que se va a divulgar, b) el interés público por el conocimiento de dicha información; c) la objetividad formal de la exposición; d) la pertinencia de la noticia de la publicación de información personal (resolución del 9 de abril de 1998, n.º 3679).

persona que ha abusado de su posición como gerente para obtener ventajas financieras en el pasado busca empleo en una situación similar». ⁴¹ El derecho al olvido también se enfrenta a dificultades con respecto a ciertos miembros de la sociedad (políticos, figuras públicas) cuya transparencia es importante desde el punto de vista de la credibilidad política ⁴² y la rendición de cuentas democrática.

De este breve análisis, yo haría dos recomendaciones. En primer lugar, no hay necesidad de reinventar la rueda con respecto a la ponderación de los intereses relacionados con el derecho al olvido. Como hemos visto, la ley ha preparado ya una serie de criterios para alcanzar este equilibrio. Lo que necesitamos ahora es transponer y adaptar estos criterios a otros casos y circunstancias en los que se puede invocar el derecho a ser olvidado. Dada la creciente digitalización de la información y el almacenamiento de nuestros actos y comportamientos más cotidianos, la aplicación del derecho al olvido (y los criterios para equilibrarlo con otros derechos) no debe limitarse a la esfera penal. La necesidad de ser olvidado es hoy una realidad que va más allá de la referencia a las posibles sentencias penales. Estas son, de hecho, solo las situaciones más extremas. Hoy en día, también una foto inoportuna en una fiesta o un *tweet* desafortunado puede descontextualizar la identidad proyectada, poniendo en peligro, por ejemplo, un futuro contrato de trabajo. El principio del olvido, que «ya se ha afirmado en algunos casos en tribunales nacionales o aplicado en sectores específicos, por ejemplo, para los archivos de la policía, los antecedentes penales o expedientes disciplinarios» ⁴³ debe ampliarse a otros casos, que pueden no ser tan extremos como los mencionados, pero que aún pueden acarrear daños y aflicciones muy importantes de la identidad personal. Así, se pueden encontrar otros criterios para la admisibilidad y el uso del derecho a ser olvidado en los plazos de prescripción establecidos en el Código civil, Código penal o en los sistemas de derecho civil (o estatuto de limitaciones en los sistemas de derecho consuetudinario). Durante el período de tiempo en que se pueden iniciar procedimientos judiciales basados en un acontecimiento particular, no se

podría ejercer el derecho al olvido de la información relacionada con ese acontecimiento. En otras palabras, el tiempo establecido para el procesamiento legal de una deuda o crimen también servirá como período durante el cual el derecho al olvido no estaría disponible. Esto significa, por ejemplo, que para los delitos graves que no prescriben, el derecho a ser olvidado nunca se podría usar. La razón de ser del establecimiento de plazos de prescripción es doble. En primer lugar, la presunta conducta ilegal debe ser tratada por los tribunales competentes, a la mayor brevedad posible tras su ocurrencia, mientras las pruebas todavía están *calientes* y no se han corrompido. En segundo lugar, las personas deben tener el derecho a continuar con sus vidas sin el peso de que sus acciones del pasado generen procesos judiciales en el presente. Esta última razón, una vez más, se puede relacionar con la necesidad de hacer eliminar restos de identidades anteriores para poder construir una nueva identidad.

Es obvio que pueden surgir nuevas situaciones que restringirán la ley para alcanzar nuevos equilibrios entre el derecho al olvido y otros derechos en competencia. La aparición de los motores de búsqueda y la creación de archivos de periódicos electrónicos en Internet -que permiten un acceso fácil, permanente y gratuito a información pasada- son solo dos ejemplos de cómo la memoria del nuevo mundo tecnológico digital sigue desafiando el derecho a ser olvidado exigiendo que se adapte y actualice de forma continua a nuevos factores y condiciones. Sin embargo, es importante tener en cuenta que ya están en marcha una serie de principios y criterios para equilibrar estos derechos en conflicto. Debemos tenerlos en cuenta y elaborar su adaptación a partir de estos principios y criterios.

En segundo lugar, creo que se debe prestar atención e investigación no solo a la dicotomía eliminación-conservación, sino también al binomio eliminación-anonimización. Mucha de la información que producimos hoy, puede ser usada para fines importantes y legítimos si no

41. Werro, 2009, pág. 291.

42. El derecho a ser olvidado, a este respecto, no debe usarse como un instrumento para que los políticos y otras figuras que ejercen puestos públicos de responsabilidad vuelvan a escribir su propia historia, buscando, por ejemplo, borrar los registros de las declaraciones de opiniones políticas que abandonaron más tarde. La aplicación de lo que podríamos llamar la *cláusula de figura pública* como una excepción al derecho al olvido es, sin embargo, un tema delicado ya que cualquiera puede (al menos en teoría) ser una figura pública.

43. SEPD, 2011, pág. 19.

se elimina. Es el caso, por ejemplo, de los sistemas públicos de vigilancia de la salud⁴⁴ y los ejercicios de prospección (concretamente, los sistemas de modelización y las plataformas de simulación basadas en procesos avanzados de minería de datos).⁴⁵ Dado que la mayoría de estos análisis y prácticas de seguimiento se pueden hacer usando datos anónimos, se debe investigar más sobre la promulgación de leyes de protección de datos que regulen y definan los objetivos para los que datos personales se pueden eliminar o anonimizar. Se debe repensar la admisibilidad incondicional de un derecho automático a ser olvidado (integrado en el diseño tecnológico y activado por defecto) y se debe meditar la posibilidad de introducir un sistema más detallado (que detalle los objetivos, condiciones y requisitos para la anonimización de los datos personales).

5. Conclusión

Hoy en día, lo que publicamos en Internet se convierte en una especie de tatuaje indeleble. El pasado ya no es el pasado, sino un presente eterno. Mayer-Schönberger sostiene que «cuanta más y más información se agrega a la memoria digital, el recuerdo digital confunde la toma de decisiones humanas sobrecargándonos con la información que más nos valdría haber olvidado».⁴⁶ Yo añadiría que el recuerdo constante de la tecnología digital también confunde las identidades, superponiendo trazas y acciones que pertenecen a una identidad que ya no queremos ver representada y recordada.

En vista de este estado de cosas, he presentado una conceptualización más esmenada y más densa del derecho a ser olvidado amparándolo en el derecho a la identidad personal. La asociación entre el derecho a ser olvidado y

el derecho a la identidad personal⁴⁷ que propongo ofrece un argumento más consistente para el surgimiento y la consolidación del derecho al olvido. Así, el derecho al olvido no solo se debe considerar desde el punto de vista de la privacidad, sino también desde el de la identidad. Por tanto, es importante reconocer no solo las consecuencias inmediatas de la aplicación del derecho a ser olvidado, es decir, la posibilidad de ocultar una serie de hechos y acciones pasadas del conocimiento público (la perspectiva de la privacidad), sino también tener en cuenta las implicaciones más profundas de la aplicación de tal derecho, es decir, lo que el derecho al olvido nos permite hacer después.

Desde esta perspectiva, he defendido que el derecho a ser olvidado no solo comparte un interés innegable en la propia singularidad y la diferencia frente a los demás, sino que también desarrolla estos intereses en una forma novedosa y sin precedentes. El derecho al olvido constituye el derecho a ser diferente no solo de los demás, sino de uno mismo, del individuo que fuimos en el pasado. El derecho al olvido, como tal, pone de relieve el proceso de deconstrucción de la identidad por el que se pueden eliminar viejas identidades y se pueden formar otras nuevas. Además, el derecho a ser olvidado también equivale al derecho a un nuevo comienzo, el derecho a empezar de nuevo desde cero y el derecho a la autodefinición, que evita que el pasado condicione (de una manera excesiva) nuestra vida presente y futura. El derecho a ser olvidado, por tanto, se considera un instrumento jurídico importante para deconstruir y reconstruir la propia identidad, para tener la oportunidad de volver a crearse uno mismo ejerciendo un mayor control sobre la propia identidad.

Sin embargo, el derecho al olvido no es, de ninguna forma, absoluto. La teorización más elaborada del derecho al olvido que he tratado de desarrollar no trata de

44. Es el caso de Epicenter, que automáticamente recopila, administra y analiza datos relacionados con la salud para ayudar a los profesionales de salud pública a detectar y responder más eficazmente a las condiciones cambiantes de salud. Véase <http://www.hmsinc.com/service/epicenter.html>.

45. Los datos de Internet, de hecho, cada vez se usan más para modelar el futuro. Un ejemplo es el mapa de salud apoyado por Google (<http://healthmap.org>), que supervisa las enfermedades infecciosas en todo el mundo mediante la síntesis de los datos públicos. Otro ejemplo es FuturICT (www.futurict.eu), un proyecto que se propone usar datos en tiempo real (transacciones financieras, registros de salud, los datos de logística, las emisiones de dióxido de carbono o bases de datos de conocimiento como Wikipedia) para construir un modelo de sociedad capaz de simular las condiciones y tendencias futuras.

46. Mayer-Schönberger, 2009, pág. 163-164.

47. En este contexto, Níger (2008a) afirma que el derecho a la identidad representa la referencia fundamental del derecho al olvido («Il diritto all'identità personale rappresenta, quindi, la matrice prima del diritto all'oblio»).

argumentar que el derecho a ser olvidado deba prevalecer siempre. La idea es simplemente argumentar que el derecho al olvido, conceptualizado y apoyado por el derecho a la identidad, presente una justificación más racional y fuerte para alcanzar un equilibrio mejor y más justo con los demás derechos e intereses.

Por otra parte, esta conceptualización particular del derecho a ser olvidado, tiene implicaciones importantes y pragmáticas. El cambio de paradigma de la privacidad a la identidad también refuerza y amplía la aplicabilidad del derecho al olvido abarcando otras áreas y situaciones que no podría abarcar de otro modo.

Referencias

- ANDRADE, N. N. G. d. (2011). «Data protection, privacy and identity: distinguishing concepts and articulating rights». En: S. Fischer-Hübner; P. Duquenoy, M. Hansen, R. Leenes; G. Zhang (eds.). *Privacy and identity management for life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School*. Helsingborg, Suecia, 2-6 de agosto 2010. Revised selected papers (pág. 90-107). Berlín y Heidelberg: Springer.
- BEAN, C. (2010). «#Posterity. How future historians will use the Twitter archives». Publicado martes 20 de abril de 2010. [Consultado 2 de octubre de 2010]. <<http://www.slate.com/id/2251429/>>
- COMISIÓN EUROPEA (CE) (2010). *Un enfoque integral sobre protección de datos personales en la Unión Europea*.
- COMISIÓN EUROPEA (CE) (2011). *Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union*.
- COMISIÓN EUROPEA (CE) (2012). *Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*. COM (2012) 11 final. Bruselas, 25.1.2012.
- DE HERT, P. (2008). «A right to identity to face the Internet of Things?» <http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf> También en el CD de la Commission Nationale française pour l'Unesco, *Ethique et droits de l'homme dans la société d'information*. Actes, synthèse et recommandations, 13-14 de septiembre de 2007, Estrasburgo.
- GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea*.
- GUTWIRTH, S. (2009). «Beyond identity?» *IDIS - Identity in the Information Society*. Vol. 1, n.º 1, pág. 122-133.
- HILDEBRANDT, M. (2006). «Privacy and identity». En: E. CLAES; A. DUFF; S. GUTWIRTH (eds.). *Privacy and the criminal law* (pág. 43-57). Amberes: Intersentia; Oxford: Hart Pub. [distribuidor].
- HILDEBRANDT, M. (2009). «Profiling and Aml». En: K. RANNENBERG; D. ROYER; A. DEUKER (eds.). *The future of identity in the information society: challenges and opportunities* (pág. 273-313). Berlín/Londres: Springer.
- MAYER-SCHÖNBERGER, V. (2009). *Delete: the virtue of forgetting in the digital age*. Princeton: Princeton University Press
- MAYES, T. (2011). «We have no right to be forgotten online». *The Guardian*, 18 de marzo.
- NEETHLING, J. (2005). «Personality rights: a comparative overview». *Comparative and International Law Journal of Southern Africa*. Vol. 38, n.º 2, pág. 210-245.

- NEETHLING, J.; POTGIETER, J. M.; VISSER, P. J. (1996). *Neethling's law of personality*. Durban: Butterworths.
- NIGER, S. (2008a). «Il diritto all'oblio». En: G. FINOCCHIARO (ed.). *Diritto all'anonimato: anonimato, nome e identità personale* (pág. 59-73). Padua: Cedam.
- NIGER, S. (2008b). «Il diritto all'identità personale». En: G. FINOCCHIARO (ed.). *Diritto all'anonimato: anonimato, nome e identità personale* (pág. 113-129). Padua: Cedam.
- PAUL-CHOUDHURY, S. (2011). «Your digital legacy». *NewScientist*, 23 de abril.
- PINO, G. (2000). «The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights». En: M. VAN HOECKE; F. OST (eds.). *The harmonization of private law in Europe* (pág. 225-237). Oxford: Hart Publishing.
- PINO, G. (2003). *Il diritto all'identità personale: interpretazione costituzionale e creatività giurisprudenziale*. Bologna: Il mulino.
- PINO, G. (2010). «L'identità personale». En: S. RODOTÁ; P. ZATTI (eds.). *Trattato di biodiritto*. Vol. 1, pág. 297-321. Milán: Giuffrè.
- POUSSON, A. (2002). «Domicile et identité. "Je t'aime, moi non plus"». En: J. POUSSON-PETIT (ed.). *L'identité de la personne humaine. Étude de droit français et le droit comparé* (pág. 529-564). Bruselas: Bruylant.
- RICOEUR, P. (1992). *Oneself as another*. Chicago: University of Chicago Press.
- ROSEN, J. (2010). The web means the end of forgetting. *The New York Times*, 21 de julio.
- SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (SEPD) (2011). *Dictamen del 14 de enero de 2011 del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - «Un enfoque integral sobre protección de datos personales en la Unión Europea»*.
- TRUCCO, L. (2004). *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*. Turín: Giappichelli.
- WERRO, F. (2009). «The right to inform v. the right to be forgotten: A transatlantic clash». En: A. COLOMBI CIACCHI; C. GODT; P. ROTT; L. JANE SMITH (eds.). «Liability in the third millenium». *Georgetown Public Law Research Paper*. N.º 2, pág. 285-300. Baden-Baden: F.R.G.
- ZITTRAIN, J. (2008). *The future of the Internet and how to stop it*. New Haven: Yale University Press.

Cita recomendada

ANDRADE, Norberto Nuno Gomes de (2012). «El olvido: El derecho a ser diferente... de uno mismo. Una reconsideración del derecho a ser olvidado». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 13, pág. 67-83. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-andrade_esp/n13-andrade_esp>

ISSN 1699-8154



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Acerca del autor

Norberto Nuno Gomes de Andrade
norberto.andrade@ec.europa.eu

Norberto Nuno Gomes de Andrade es investigador científico de la Unidad de Sociedad de la Información del Instituto de Estudios Tecnológicos Prospectivos (IPTS) del Centro Común de Investigación de la Comisión Europea e investigador jurídico del Departamento de Derecho del Instituto Universitario Europeo (EUI, Italia). Sus intereses de investigación se centran en el derecho y la tecnología (en particular, la biotecnología, la neurociencia y la inteligencia artificial), la legislación sobre protección de datos y privacidad. En el 2009, coeditó y publicó *Law and Technology: Looking into the Future - Selected Essays*.

Comisión Europea
IPTS, Unidad de Sociedad de la Información
Edificio Expo
C / Inca Garcilaso, 3 - 2º piso
41092 Sevilla, España

<http://idp.uoc.edu>

Monográfico «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet»

ARTÍCULO

Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido

Javier de la Cueva González-Cotera

Fecha de presentación: noviembre de 2011

Fecha de aceptación: noviembre de 2011

Fecha de publicación: febrero de 2012

Resumen

Los días 11 y 12 de julio del 2011 se celebró en Barcelona el VII Congreso Internacional sobre Internet, Derecho y Política que se centró en los dos temas principales de la neutralidad de la red y el derecho al olvido. Además de estos contenidos, se expusieron por parte de sus autores ponencias relacionadas con la última problemática jurídica y política cuyo objeto es Internet. En este artículo se realiza una crónica no exhaustiva del congreso, incluyéndose las conclusiones del relator a la finalización de cada jornada.

Palabras clave

neutralidad de la red, derecho al olvido, derecho de información, libertad de expresión

Tema

Derecho

Report of the 7th International Conference on Internet, Law and Politics: Net Neutrality and the Right to Oblivion.

Abstract

The 7th International Conference on Internet, Law and Politics was held in Barcelona on 11 and 12 June 2011, focusing on the two main topics of net neutrality and the right to oblivion. Several authors also presented papers on current problems of the Internet from a legal and political standpoint. This article is a non-exhaustive report on the conference and includes the conclusions given by the conference secretary at the end of each day.

Keywords

net neutrality, right to oblivion, right to information, freedom of expression

Topic

Law

Introducción

Durante los dos días consecutivos que duró la celebración del congreso,¹ tuvimos la oportunidad de atender a dos conferencias y a ocho mesas redondas. Un total de 40 intervinientes, a los que debemos añadir los moderadores de las diferentes sesiones, realizaron aportaciones de altísima calidad y radical actualidad sobre los dos temas que vertebraron el congreso: la neutralidad de la red, que fue objeto de las sesiones del primer día, y el derecho al olvido, que ocupó la segunda jornada.

Además de estas líneas principales, dado que el objeto temático «Internet, Derecho y Política» de los sucesivos congresos (del que este ha sido la séptima edición) no es trivial sino que hace referencia a las trascendentales transformaciones en las que se hallan inmersas las sociedades actuales, asistimos a variadísimas intervenciones de las que quedó un consenso tácito sobre el hecho de que nos hallamos en plena transformación de una era histórica a otra en una transformación de tal magnitud como lo pudo ser el paso de la Edad Media a la Edad Moderna, comenzando a vislumbrar nuevos problemas jurídicos de los que la neutralidad de Internet y el derecho al olvido son dos simples ejemplos de los muchos que nos encontraremos. Lo tratado en el congreso evidenció que el derecho es un constructo vivo que debe replantearse sus cimientos en los campos de la teoría del derecho, en lo referente a la extensión de la norma jurídica y su interrelación con el código informático de la filosofía del derecho sobre si los artefactos tienen ideología, y la Justicia que entonces cabría aplicar, y de la sociología del derecho en cuanto a la ineficacia de las normas jurídicas derivada de las múltiples jurisdicciones, legislaciones aplicables y

naturaleza digital del objeto informacional. No está de más aclarar que esta enumeración no agota la pluralidad de problemas detectados.

Los agentes intervinientes

Una de las dificultades detectadas por numerosos participantes en el congreso² ha sido la relativa a los agentes intervinientes bien como sujetos titulares de derechos y obligaciones, bien como terceros intermediarios. Tanto la neutralidad de la red como la información objeto del derecho al olvido se manifiestan en un espacio topológico complejo constituido por múltiples nodos que operan bajo el régimen de cliente-servidor y cuya información, como bien sabemos, se transmite a través de muy variados sistemas de comunicación (cables, ondas) que atraviesan diferentes jurisdicciones en cada una de las cuales existe una legislación diferente.

A esta ya conocida complejidad, cuyas relaciones resultantes son objeto de estudio por el derecho internacional privado, debe actualmente sumarse una nueva problemática nacida de los siguientes sujetos intervinientes:

- Existencia de múltiples agentes técnicos y jurídicos intervinientes en la denominada *cloud computing*. La evolución de los servicios de Internet hacia plataformas donde la información se desconoce dónde se halla físicamente almacenada, los sistemas técnicos de balanceo de cargas entre diferentes ordenadores y el almacenamiento virtual hacen prácticamente imposible conocer todas las jurisdicciones y leyes aplicables. Esta cuestión plantea problemas del lugar de ejecución de la acción.

1. El programa del congreso se halla en la URL: <http://edcp.uoc.edu/symposia/idp2011/programme/> [documento en línea]. Fecha de última consulta 23 de noviembre de 2011.

2. Puede accederse al libro de actas del congreso, donde se incluyen todas las comunicaciones, en la URL: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8341/7/IDP_7.pdf [documento en línea]. Fecha de última consulta: 23 de noviembre del 2011.

- Intervención en las infraestructuras de nuevos agentes colectivos y distribuidos, de los que son ejemplo las redes sociales N-1,³ la todavía en fase alfa Diáspora,⁴ o la ya bien implantada infraestructura de Guifi.net,⁵ que conecta sin pasar por un proveedor de servicios tradicional 14.798 nodos en la fecha de redacción de este artículo, pudiendo articularse como los usuarios deseen, puesto que se trata de una organización horizontal no jerarquizada.
- La existencia de agentes colectivos autoorganizados, que intervienen en los contenidos, como por ejemplo los editores de Wikipedia, o los desconocidos que se agrupan bajo la denominación genérica de *anonymous* y que suponen grupos de personas titulares de derechos y obligaciones pero cuyas relaciones jurídicas son difíciles de individualizar en casos de responsabilidad o de infracciones.

Ya no se trata, por tanto, de una dificultad derivada de la existencia de múltiples jurisdicciones y legislaciones aplicables, sino de la identificación de los sujetos relevantes para una correcta configuración de los haces de derechos y obligaciones que suscita operar en Internet como veremos en lo referente a la neutralidad de la red y en el derecho al olvido. Por otra parte y siguiendo un criterio utilitarista, la imposibilidad de procedimientos cautelares ante las conductas descritas impone la preeminencia de un derecho reparador sobre el preventivo.

Neutralidad de Internet

La neutralidad de la red puede ser definida como el principio que garantiza que todo contenido que se transmite por una red de comunicaciones es tratado de la misma manera y sin discriminación alguna ni por su contenido ni por su origen o destino. La conferencia inaugural de la jornada dedicada a este tema fue dictada por Christopher T. Marsden,⁶ autor de la obra *Net Neutrality: Towards a Co-Regulatory Solution*⁷ quien, realizando un análisis del

pasado, presente y futuro de la neutralidad de Internet, comenzó su exposición recordando que el debate sobre la neutralidad es antiguo y se remonta a la 1844 Railway Act del Reino Unido que reguló unas condiciones mínimas en el transporte de viajeros por ferrocarril. La imposición de unas condiciones mínimas se fundamenta en lo que en derecho de competencia se entiende bajo el acrónimo FRAND, *fair, reasonable, and non-discriminatory terms*, lo que supone en la práctica unos estándares comunes a ser aplicados en unos bienes o en la prestación de servicios para asegurar la compatibilidad entre los diferentes operadores económicos concurrentes en un mercado. El ejemplo histórico más claro fue la adopción de un mismo ancho de vía por las empresas ferroviarias.

En 1999 se introdujo el debate de la neutralidad de la red en una Internet que hasta entonces se regía por el *common carriage* basado en FRAND y que en el Reino Unido operaba sobre cuatro aspectos: la interoperabilidad, la interconexión, la privacidad y la interceptación. En EE. UU. esta neutralidad tenía en cuenta el derecho a utilizar cualquier aparato o aplicación para el servicio de recepción de contenido, la no discriminación, la transparencia y el análisis casuístico de las diversas situaciones de hecho que pudieran darse. Las regulaciones norteamericanas de la Federal Communications Commission (FCC), canadiense de la Canadian Radio-television and Telecommunication Commission (CRTC) y europea de la Comisión de la UE, introdujeron unos principios vagos de neutralidad de la red, estableciéndose como solución un sistema débil consistente en que «si tu proveedor te bloquea Skype, cámbiate de proveedor». De esta manera, los sistemas censores se apartaban de los poderes públicos para caer en manos de las empresas privadas. En la actualidad, existe derecho positivo sobre la neutralidad de la red en Chile, Finlandia y Holanda, así como un sistema de corrección en Noruega.

El profesor Marsden señaló en su conferencia que el contexto del futuro para el establecimiento de una neutralidad

3. Disponible en: <https://n-1.cc/> [documento en línea]. Fecha de último acceso: 23 de noviembre del 2011.

4. Disponible en: <https://joindiaspora.com/> [documento en línea]. Fecha de último acceso: 23 de noviembre del 2011.

5. Disponible en: <http://guifi.net/> [documento en línea]. Fecha de último acceso: 23 de noviembre del 2011.

6. Profesor de la Universidad de Essex (Reino Unido). Página personal en la web de la Universidad de Essex: <http://www.essex.ac.uk/law/staff/profile.aspx?ID=832> [documento en línea]. Fecha de última consulta 23 de noviembre del 2011. Blog: <http://chrismarsden.blogspot.com/> [documento en línea]. Fecha de última consulta 23 de noviembre del 2011.

7. C. Marsden (2010). *Net Neutrality: Towards a Co-Regulatory Solution*. Londres: Bloomsbury Academic.

de la red se encuentra con una situación en la que el modelo está roto, la Unión Europea no lidera su imposición, los proveedores de acceso no invierten en las redes y éstas son un desorden (*broadband is a mess in Europe*). Finalizó afirmando que necesitamos normas sobre qué pueden y no pueden hacer los proveedores de servicios de Internet, ya que nos hallamos ante cuestiones de derechos fundamentales y no de derecho de la competencia, lo que conlleva dramáticas implicaciones.

En la mesa redonda sobre las opciones de política legislativa, intervinieron los ponentes Antoni Elías,⁸ Joan Barata⁹ y Angel León,¹⁰ señalándose por Antoni Elías las complejidades técnicas, legales, económicas y su carácter de «sutil y complicado motor social» de Internet, debiéndose pensar a nivel global y propugnándose un organismo más allá de ICANN que se encargase de la gobernanza de la red. Se ha disparado el tráfico y a nivel económico no queda claro que la tarificación pueda satisfacer las necesidades de financiación para la modernización de las infraestructuras y si bien las operadoras de telefonía móvil no respetan la neutralidad de la red, los proveedores habituales deberán seguir con el carácter abierto y neutral.

Para Joan Barata, la discusión sobre la neutralidad de la red no es tecnológica sino una tensión entre la autorregulación y la regulación externa. La problemática se amplía con la existencia de agentes como los buscadores, cuya posibilidad de pago es evidente y si bien parecería evidente que quien más pagase habría de tener un mejor servicio, existiría otra cuestión a dilucidar sobre si el pago pudiera ser diferente en función del tipo de contenido. Los EE. UU. y la UE se aproximan desde diferentes perspectivas a esta cuestión, manteniendo ya la FCC unos puntos sobre el debate: (i) requerimiento regulatorio de transparencia de los proveedores de acceso a Internet tanto en relación con el usuario final como frente a terceros actores en la red para el desarrollo de aplicaciones y servicios; (ii) no bloqueo de aplicaciones y contenidos de terceros en virtud del principio clásico de la libre competencia en el mercado; (iii) prohibición de llevar a cabo una

discriminación que no sea razonable, no siéndolo discriminar por motivos de dominio de mercado, de libertad de expresión o por pago, quedando la duda si la discriminación se solicita por el usuario por motivos, por ejemplo, de ludopatía y sí siendo razonable la discriminación por motivos de tráfico no deseado y congestiones de red.

El último de los ponentes, Angel León, mantuvo una actitud crítica con el enfoque normativo por «sus grandes lagunas». En las actuales propuestas se plantean objetivos de conectividad entre los extremos, la defensa de los derechos fundamentales (las redes son un vehículo para su ejercicio) y garantizar que no existan infracciones contra la libre competencia, objetivos que según el ponente tienen 20 años de antigüedad. La neutralidad de la red es un concepto unificado, puesto que integra los objetivos señalados, un concepto específico de las telecomunicaciones que ahora se aplica a los proveedores de servicios de Internet, y es un concepto genérico, ya que su exigencia lo es para todos los operadores. No obstante, en el enfoque actual existen unas diferencias con respecto al enfoque tradicional: (i) un criterio de mínima intervención regulatoria, (ii) excepciones para los servicios móviles y (iii) si bien la neutralidad de la red se enfoca en el bucle del abonado, se puede atentar contra la misma a lo largo de muchos más elementos de la cadena de transmisión de la información.

Sobre la neutralidad de la red, siguió una mesa redonda en la que se abordó el concepto desde el punto de vista de los operadores, proveedores de contenido y usuarios, con la intervención de Maite Arcos,¹¹ Andreu Teixidor¹² y Ofelia Tejerina.¹³ Por parte de la representante de las operadoras, se dio únicamente una perspectiva económica, definiéndose Internet como un ecosistema en el que las empresas entran para ganar dinero. RedTel invierte en sus propias redes y los agentes que operan en las mismas son los proveedores de contenidos (que se financian con publicidad), proveedores de servicio (lo hacen por pagos de sus abonados) y facilitadores de servicios (Paypal, que se financia por comisiones). En definitiva, el usuario final

8. Catedrático de la Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona, Universidad Politécnica de Cataluña.
9. Profesor de Derecho de la Comunicación y vicedecano de Relaciones Internacionales y Calidad de la Facultad de Comunicación Blanquerna, Universidad Ramon Llull.
10. Dirección General de Telecomunicaciones y Sociedad de la Información del Ministerio de Industria, Turismo y Comercio.
11. Directora General de RedTel.
12. Director de estrategia editorial de BUBOK.
13. Abogada de la Asociación de Internautas.

acaba pagándolo todo. Este círculo virtuoso, sin embargo, y según la ponente, queda alterado porque el actual tráfico no genera los suficientes ingresos para financiar las redes, por lo que para conservar el carácter abierto e innovador se necesita una financiación adicional. El debate, por tanto, no es de libertades fundamentales y derechos humanos, sino económico.

Andreu Teixidor relató su experiencia desde la editorial de libros tradicional a la edición por demanda e incidió en los valores filosóficos y de cambios profundos sociales a los que asistimos y que nos esperan. Reivindicó el derecho de todo ciudadano al acceso en igualdad de condiciones los contenidos de la red, hallándose la sociedad en situación crítica y en duda los modelos de Estado y propiedad intelectual. La neutralidad de la red, para este ponente, ha de ser garantizada públicamente.

La abogada Ofelia Tejerina, interviniente última, puso el acento en que Internet se hace por los usuarios, debiéndose ofrecer a los mismos la libertad de elección, unos mínimos de calidad a un precio razonable y un principio de intervención mínima del Estado en las redes, debiendo su actividad limitarse a la vigilancia del precio y del acceso.

Derecho al olvido

En la segunda jornada del congreso, el derecho al olvido fue introducido y definido por Esther Mitjans¹⁴ como «el derecho a que el pasado no se convierta en presente continuo». La profesora Mitjans resaltó no sólo el valor jurídico del concepto sino también el aspecto vital de la necesidad de olvidar el pasado, si bien ello no implica la necesidad de cambiar la historia. El derecho al olvido es una cuestión global y, por tanto, se necesitan unos principios globales, dudándose todavía en su construcción doctrinal de si se trata de un derecho nuevo del usuario y de un deber de los proveedores de los contenidos a no tener nuestros datos por siempre. La posibilidad de retirar contenidos no estaba prevista por la legislación ni por la

doctrina y tras la aparición de los buscadores de Internet, habremos de responder a las preguntas de cómo puede regularse esta materia.

Por su parte, Cécile de Terwangne,¹⁵ que dictó la conferencia titulada «Privacidad en Internet y el derecho al olvido», señaló que se trata del derecho de las personas físicas a que sea borrada tras un cierto tiempo la información referida a ellas. La profesora Terwangne señaló que la autonomía individual de la persona implica que esta tenga poder y pueda controlar su propia información personal, lo que tiene dos vertientes: a quién se desea entregar información y de quién se desea que ya no disponga de la misma. La información de la que hablamos no es la limitada a la privacidad, sino toda aquella relacionada con una persona física como por ejemplo la información profesional o comercial. Europa ya ha reconocido este derecho a la autodeterminación informacional en el artículo 8 de la Convención Europea de Derechos Humanos, en el Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en el artículo 8 de La Carta de los Derechos Fundamentales de la Unión Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En el ejercicio del derecho al olvido se generan conflictos con el derecho a la información, ya resueltos por los tribunales, que han utilizado para tomar una decisión los criterios del tiempo transcurrido y de la noticiosidad de la información, estableciéndose también dos excepciones: los hechos históricos y los ligados a las figuras públicas. La casuística que aparece en el ejercicio de este derecho ha de ser resuelta caso por caso, encontrándonos con supuestos de información distribuida o de su exposición concentrada, anonimización en bases de datos y casos de periódicos digitales.

En sus conclusiones, la ponente expuso que este derecho ya ha sido reconocido judicialmente y que implica bien el borrado o la anonimización de la información, bien la objeción al procesamiento de la información, debiendo cuidarse la restricción de los derechos a la información y

14. Directora de la Agència Catalana de Protecció de Dades y profesora de Derecho Constitucional de la Universidad de Barcelona, que moderó la primera mesa redonda de la segunda jornada.

15. Profesora del Centre de Recherche Informatique et Droit (CRID). Página personal: http://www.fundp.ac.be/universite/personnes/page_view/01002526/ [documento en línea]. Fecha de última consulta: 23 de noviembre del 2011.

libertad de expresión, la obligación de retener datos por cuestiones de seguridad, la posibilidad de establecer un derecho al borrado de la información y no sólo a hacerla inaccesible y la posibilidad de ampliar el existente derecho al olvido a un derecho automático de ser borrado por defecto.

En la primera mesa redonda sobre la neutralidad de la red, intervinieron Norberto Nuno Gomes de Andrade,¹⁶ Milagros Pérez Oliva,¹⁷ María González Ordoñez¹⁸ y Ricard Martínez Martínez.¹⁹ Para el primero de los ponentes, es necesario profundizar en un concepto que ha de ser ligado más con el derecho a la identidad personal que a la privacidad, concepto sobre el que existe un amplio consenso que ha de ser respetado. Se trata de una figura jurídica que triangula entre la protección de datos, la privacidad y la identidad, pero que su encuadramiento bajo la identidad tiene las ventajas siguientes: refuerza la narrativa de la identidad, correspondería a una parcela del derecho en expansión, concuerda con la ratio del derecho a la identidad personal de no ser representada falsamente, cubre los hechos que ya se hallan publicados y evita requisitos de veracidad en la información no contextualizada.

Milagros Pérez Oliva, en su condición de defensora del lector de *El País* aportó una rica variedad de supuestos, realizando una aproximación práctica al derecho al olvido. Incidió en la colisión entre el derecho a la privacidad y el derecho a la información, del que mencionó que los periódicos no son los titulares del derecho sino los depositarios. El hecho de que la información se halle a disposición de los ciudadanos es un servicio público, existiendo en la actualidad el problema de la nueva visibilidad que Internet permite y enumeró la siguiente casuística: drogadicto ya rehabilitado que aparece en una noticia; cirujano imputado por mala praxis y que finalmente fue absuelto; joven que participó en un foro antisistema; gimnasta que nunca tuvo un caso de anorexia pero que así se había extendido por la red; niña que hace 25 años presencié la muerte de su madre a manos de su padre; joven abogado que sufre las consecuencias de una noticia de una estafa por la que condenaron a su hermana; persona

en Buenos Aires que sufre las consecuencias de una noticia en la que se narra su imputación como colaborador de ETA sin que se indique el resultado del procedimiento penal.

Señaló Milagros Pérez Oliva que los archivos han de estar a disposición de los ciudadanos sin modificar, debiéndose reflexionar sobre cuándo una noticia ya no es relevante y quién decide sobre su vigencia, categorizando las noticias en cuatro grupos:

- Noticia verídica publicada legítimamente pero cuyas circunstancias cambiaron posteriormente.
- Noticia verídica pero negativa.
- Noticia verídica pero incompleta, donde el lector nunca sabrá el final.
- Noticia falsa o errónea no rectificadas en su momento.

La representante de Google, María González Ordoñez, repasó dos tendencias que han encontrado en la problemática de los buscadores: un derecho al olvido que otorga al propio usuario el control efectivo sobre sus datos y otro, más amplio, que es el que garantiza que el usuario tenga la posibilidad de retirar la información que se refiere a otra persona. Afirmó en su exposición que Google es un intermediario de la sociedad de la información y que en virtud de su naturaleza goza de exención legal de responsabilidad, al ser simplemente un espejo. Señaló que Google respeta el estándar del archivo robots.txt y siempre retira la información si la fuente primaria la retira.

Por último, Ricard Martínez se refirió a los conflictos de los boletines oficiales, periódicos y buscadores, e incidió en que un derecho fundamental expresa necesidades humanas básicas. El derecho ha de interpretarse históricamente y ha de ser la tecnología quien, en el contexto actual, ha de respetar el derecho y no ajustarse el derecho a la tecnología, siendo muy parcas las posibilidades de un ciudadano en lo referente al derecho al olvido puesto que sólo goza de las posibilidades de oponerse y cancelar sus datos. Defendió un criterio de expurgo, quitar lo no relevante, y concluyó afirmando que lo que está

16. Director científico en el Instituto de Estudios Tecnológicos Prospectivos de la Comisión Europea.

17. Defensora del lector del diario *El País*.

18. Directora de la Asesoría Jurídica de Google para España y Portugal.

19. Profesor de Derecho Constitucional. Universidad de Valencia.

en juego no es el derecho de un solo individuo sino el de la colectividad.

Para finalizar el presente artículo, deseo señalar que la limitación de su extensión implica omisiones que no signi-

fican falta de relevancia de los ponentes que intervinieron o los temas que trataron. Para los demás contenidos, he de remitirme a las Actas del Congreso, de las que deseo que el presente artículo haya servido de un buen complemento e introducción.

Cita recomendada

DE LA CUEVA GONZÁLEZ-COTERA, Javier (2012). «Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 13, pág. 84-90. UOC. [Fecha de consulta: dd/mm/aa].

<<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-cueva/n13-cueva>>

ISSN 1699-8154



Los textos publicados en esta revista están -si no se indica lo contrario- bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Acerca del autor

Javier de la Cueva González-Cotera

<http://javierdelacueva.es>

Javier de la Cueva (Madrid, 1962) trabaja como abogado. En sus manos ha estado la defensa, entre otros, de Ladinamo (primera sentencia que reconoció el Copyleft), de Sharemula (que confirmó que las webs de enlaces a archivos en redes p2p no cometen delitos). Creador e impulsor de los procedimientos libres, cuyo primer procedimiento fue la demanda contra el canon en los soportes digitales, se dedica en la actualidad, además de a su trabajo como abogado, a programar diversos proyectos, como el Proyecto Kelsen (*framework* de gestión de información jurídica bajo licencia AGPL), la Ontología jurídica libre, a mantener el catálogo de Opengov.es o a diseñar Praeter Orwell. Asimismo, es profesor en el máster de Economía Digital e Industrias Creativas de la Escuela de Organización Industrial, conferenciante, usuario de GNU/Linux desde 1998 y administrador de sistemas bajo dicho sistema operativo desde el 2003. Escribe sus *scripts* en Python.

C/ Reina Mercedes, 20
28020 Madrid, España