

## Deep Packet Inspection & Co: la preocupación por el control de Internet

Miguel Gil\*

Analista asociado  
ENTER-IE

Dentro del debate sobre la *Net Neutrality* cabe preguntarse cómo los operadores podrían priorizar el tráfico en sus redes, bajo qué mecanismos y con qué implicaciones.

Diversas voces entre los defensores de la llamada neutralidad (por ejemplo, Vinton Cerf de Google) se han manifestado en contra de una práctica llamada *Deep Packet Inspection*. ¿Qué es? ¿Por qué es tan importante? ¿Qué implica su uso?

La llamada *Deep Packet Inspection* consiste en infiltrarse dentro de las distintas capas de los paquetes de información IP, lo que plantea cuestiones sobre los límites en cuanto a la privacidad de los usuarios.

Parece evidente el derecho de los operadores de telecomunicaciones a gestionar y rentabilizar sus redes (además de asegurar su mantenimiento), pero ¿hasta donde llegaría este derecho? Lo que se debate es si éste va más allá del acceso y engloba también a lo que circula dentro de esas redes. Pero sobre todo, ¿dónde están los límites de esas prácticas?

Aunque hay que saber diferenciar entre el debate sobre prácticas de gestión de tráfico en Internet por parte de los operadores (con fines comerciales o de gestión de la red), del control por parte de gobiernos y empresas, en el fondo subyace una misma preocupación: la privacidad de los usuarios en su actividad en la red y la búsqueda de garantías para tener acceso a todos los recursos que hoy en día ofrece Internet al menor precio posible.

Recientes situaciones en China, Irán, Emiratos Árabes Unidos y Rusia han alertado a la opinión pública mundial sobre los intentos de control de Internet.

Internet es hoy en día una herramienta básica para, entre otras cosas, la formación de la opinión pública y permite a sus usuarios encontrar con facilidad fuentes de información distintas a las oficiales. El hecho de que conforme una realidad paralela fuera del control de gobiernos autoritarios (y otros, no tanto), empuja a éstos a buscar la forma de controlar el uso de Internet de sus ciudadanos.

Parece que, hasta ahora, con poco éxito; hecha la limitación, hecha la trampa: en cuanto aparece una nueva forma de control, aparece a su vez la manera de evitarla.

A día de hoy, el control de la actividad de los usuarios se hace bien sobre las páginas o contenidos que visita en Internet, evitando ciertas páginas; sobre los paquetes de información que intercambian los usuarios en Internet; y, finalmente, a través de los aparatos (ordenadores o terminales móviles), instalando *software* con la connivencia o no de los fabricantes.

El objetivo de esta nota no es decantarse a favor de una u otra de las opiniones en presencia en el debate enconado sobre las prácticas de los operadores, sino ofrecer elementos de análisis que puedan ser de alguna utilidad para una reflexión necesaria.

\* El autor trabaja en la Dirección General de Sociedad de la Información de la Comisión Europea. Las opiniones expresadas en este artículo son propias al autor y no reflejan necesariamente la posición de la Comisión Europea.

En primer lugar, hay que tener en cuenta que Internet es originalmente una tecnología que se diseñó para conectar unos cuantos ordenadores universitarios y que ha crecido hasta comunicar a millones de personas en el mundo. Se trata de un sistema dinámico en constante evolución. En su momento no se dio ninguna atención a la calidad del servicio; todos los paquetes eran tratados de la misma forma.

## ¿Qué es Deep Packet Inspection?

Se conoce como *Deep Packet Inspection*<sup>1</sup> (DPI, también llamada *Complete Packet Inspection* o *Information eXtraction IX*) a una forma de filtrado de paquetes de red que examina la parte de datos y también, en la mayoría de los casos, el encabezamiento (*header*) de un paquete cuando pasa por un punto de inspección, buscando algún elemento del protocolo que no cumpla con ciertos requisitos, virus, *spam*, intrusiones o cualquier otro tipo de criterio predefinido, con el objetivo de decidir si el paquete puede pasar o si debe ser dirigido a un destino distinto.

Se trata de un procedimiento más profundo que otros como la llamada *Stateful Packet Inspection*, que simplemente analiza y clasifica basándose en el encabezamiento del paquete.

La DPI permite, por lo tanto, adentrarse en los paquetes de información en Internet (por ejemplo contenidos de un email, páginas web visitadas, archivos intercambiados).

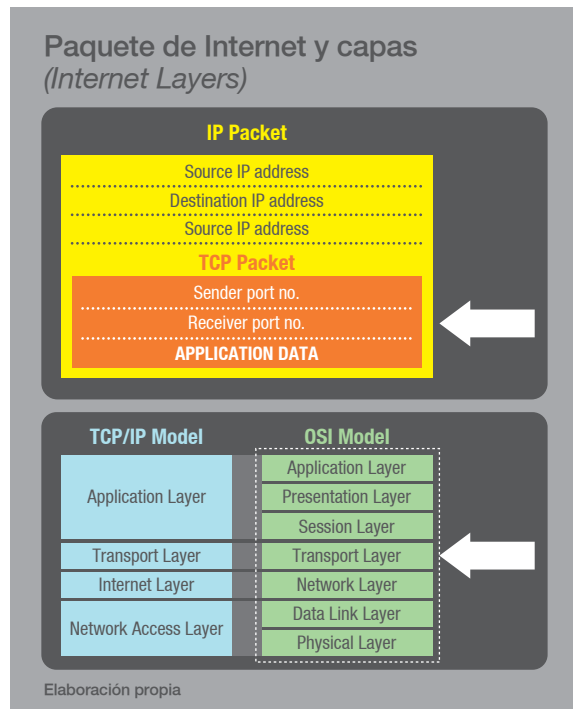
Los objetivos al utilizar la DPI pueden ser varios:

- Realizar funciones avanzadas de seguridad como la minería de datos (*Data Mining*).
- Desconexión de ciertas direcciones IP.
- Desconexión de ciertas aplicaciones.

<sup>1</sup> [http://en.wikipedia.org/wiki/Deep\\_packet\\_inspection](http://en.wikipedia.org/wiki/Deep_packet_inspection)

## ■ Cómo funciona

Los sistemas de DPI tienen la capacidad de infiltrarse en las capas 2 a 7 de modelo OSI (ver tabla más abajo). Esto incluye la cabecera (*headers*) y los protocolos de datos, así como los datos propiamente dichos (*payload*) de los paquetes.



El sistema identifica y clasifica el tráfico basándose en la información contenida en la parte de datos del paquete. Una vez clasificado, el paquete puede ser redirigido, bloqueado discriminado frente a otros dentro de la red.

Sistemas menos sofisticados de DPI identifican flujos de tipos de paquetes (P2P, por ejemplo) en vez de paquetes individuales, permitiendo acciones de control basadas en la acumulación de información de estos flujos.

## ¿Quién la realiza?

Las técnicas de DPI son utilizadas actualmente por empresas, proveedores de servicios en Internet (operadores) y gobiernos (este aspecto será tratado en mayor profundidad en el último punto de la nota).

Por ejemplo, debido a los crecientes peligros de la 'ciberseguridad', y el paso a la 'nube' con la *Cloud Computing*, cada vez más empresas instalan sistemas de DPI para proteger todas las capas de sus comunicaciones ya que, por ejemplo, los *firewalls* tradicionales no permiten distinguir entre usos de ciertas aplicaciones.

En cuanto a los operadores, sus razones serían variadas:

- Interceptaciones legales de las comunicaciones para combatir el crimen.
- Publicidad segmentada al usuario.
- Calidad del servicio (discriminar el tráfico de usuarios intensivos para que la experiencia media de los usuarios sea satisfactoria).
- Discriminación de ciertos servicios en favor de otros propios al operador.
- Protección de los contenidos sujetos a derechos de autor.

La mayoría de los operadores tienen un contrato en el que se especifica la calidad del servicio que se suministran a todos los clientes (las descargas de unos pocos no pueden hacer que el servicio de la mayoría se resienta) y unas condiciones de uso aceptables (con respecto a los contenidos protegidos por cuestiones de derechos de autor).

### ■ Interceptaciones legales de las comunicaciones para combatir el crimen

Por razones de seguridad y combate al crimen, los ISPs están obligados en los distintos Estados a ser capaces de interceptar tráfico. En algunos países, la ley obliga incluso a los operadores a realizar filtrado sobre los paquetes de los usuarios.

### ■ Publicidad segmentada al usuario

Los operadores son capaces de controlar los hábitos de navegación de sus clientes

y pueden administrar la información sobre sus intereses. Esto puede ser a su vez utilizado por compañías que lleven a esta publicidad segmentada al usuario<sup>2</sup>.

En Europa (Reino Unido), BT ha admitido haber probado esta tecnología sin el consentimiento o conocimiento por parte de sus usuarios.

### ■ Calidad de servicio (argumento preferido de los operadores)

Las aplicaciones de P2P se utilizan para el intercambio de archivos entre ordenadores.

Estos archivos, si incluyen video, pueden ser de un tamaño considerable incrementando la necesidad de capacidad de la red.

Una solución es suministrar una mayor capacidad de la red, otra discriminar el tráfico de los usuarios más intensivos en beneficio de la mayoría.

Los operadores sostienen que una minoría de los usuarios genera la mayoría del tráfico P2P y degrada la experiencia de la mayoría de los usuarios que simplemente usan el email o navegan en Internet.

Según los operadores, esto tiene como consecuencia negativa un incremento en las quejas de los usuarios y, por lo tanto, una posible pérdida de ingresos.

La DPI permitiría a los operadores asignar un volumen equitativo de ancho de banda para todos los usuarios, eliminando la posibilidad de congestión.

Además, una mayor prioridad puede ser asignado a la VoIP y a los servicios de 'videoconferencia' que requieren una menor latencia frente a otros servicios en los que la latencia no es tan determinante (email).

Sin embargo, cabe preguntarse si la profundidad en las acciones de la DPI son las mejores tecnologías para estas actividades.

<sup>2</sup> Las compañías americanas especializadas en estas tecnologías son NebuAd, Front Porch y Phorm.

## ■ Potenciación de servicios asociados

La DPI puede ser utilizada por operadores móviles para diferenciar entre los servicios que forman parte de sus 'walled gardens' y otros en Internet. De este modo, la discriminación les permitirá cobrar por los distintos servicios dentro de Internet, segmentando las ofertas al usuario e incrementando de este modo los ingresos.

## ■ Protección de contenidos sujetos a derechos de autor

Algunas legislaciones obligan a los proveedores de servicios de Internet a acciones para la protección del *copyright*. Los propietarios de derechos de autor (representados por asociaciones como la IFPI) consideran que se podría utilizar la DPI para conocer qué descarga exactamente cada usuario y si la descarga respeta o no los derechos de autor.

Se entra aquí en un punto fundamental de debate: ¿Se justifica la protección de los derechos de autor a costa de la privacidad y el secreto de las comunicaciones? ¿Es un modelo basado en la DPI sobre material descargado sostenible?

La privacidad es un derecho consagrado y los operadores deben mantener correctamente informados a los usuarios según el marco regulatorio.

## ¿Cuales son los argumentos a favor y en contra? ¿Qué implicaciones tiene a nivel económico y social?

### ■ Tráfico en la red

Como si de confirmar la regla de Pareto se tratara, unos pocos usuarios intensivos en su uso concentran la gran mayoría del tráfico.

En el caso de la banda ancha móvil, AT&T informó este año que el 3% de sus usuarios con iPhone representan el 40% del tráfico en sus redes.

¿En qué consiste este tráfico que concentra la mayoría de los recursos? Principalmente video e intercambio de archivos en redes P2P (aunque esta tecnología está en descenso debido a las mayores velocidades de banda ancha y al consiguiente ascenso del *streaming*).

### ■ ¿Congestión en la red?

Lo que dice Vint Cerf es que los operadores no deben utilizar estos sistemas con la excusa de evitar la congestión de la red. Para evitar esta situación, Cerf cree que hay que tratar la capacidad de la red como un bien escaso y, por lo tanto, darle un precio acorde con el consumo de cada usuario. Las tarifas planas en la mayoría de los casos no alcanzan jamás las velocidades anunciadas.

Se trataría de contratar velocidades y capacidades garantizadas de acuerdo con el uso, de modo que los usuarios con mayor uso de la red (ya sea por video o uso de redes P2P) sean los que más paguen, frente a los que utilizan únicamente servicios básicos en la red (como el email).

Evidentemente, estas propuestas de Google suponen un cambio con respecto al modelo actual, donde unos usuarios subvencionan a otros que, de hecho, podrían consumir más teóricamente, pero no lo hacen.

De este modo, los operadores cobrarían por el uso efectivo y los precios justificarían las mejoras en la red de acuerdo con la demanda (probablemente, los precios subirían).

### ■ Legitimidad de los operadores de telecomunicaciones

Los operadores, por su parte, declaran que están legitimados para efectuar estas prácticas para dar un mínimo servicio aceptable

para la mayoría de los usuarios en el caso de congestión de la red.

Sin embargo, también hay otra razón: los operadores han visto como las tasas de crecimiento de sus ingresos disminuían en los últimos ejercicios y deben buscar nuevas fuentes de ingresos. No quieren quedarse simplemente como suministradores de acceso y les interesaría poder cobrar por los contenidos en Internet, discriminando por el tipo de tráfico.

De todos modos cabe preguntarse si después de tantos años de un acceso a los recursos de Internet casi ilimitado, tendrían éxito ofertas de banda ancha con y sin Facebook, o en las que las búsquedas en Google estuvieran sujetas a distintas velocidades. ¿Tiene esto sentido?

Existe un problema de información asimétrica: sólo los operadores saben lo que sucede realmente en sus tramos de red. El resto de los ciudadanos sólo se pueden fiar cuando señalan problemas de congestión e Internet es un conjunto de redes fragmentadas.

Basarse simplemente en la buena fe de los operadores no parece la mejor solución. Es por ello que serían necesarias unas reglas claras y compartidas.

## ■ DPI y la *Net Neutrality*

Las organizaciones de usuarios preocupadas por los principios de la *Net Neutrality* consideran que el análisis de las capas de contenidos dentro de un paquete IP no es apropiado y que puede afectar de manera determinante a la privacidad del usuario. Algo irónico y algo cómico ya que algunas compañías de Internet que se ponen del lado de estas asociaciones de internautas basan su negocio en todo tipo de datos privados.

Las operadoras consideran que la adopción de los principios de la *Net Neutrality* puede hacer que los operadores no tengan ningún incentivo para mejorar las redes: al

no poder discriminar el tráfico, pierden un modelo de negocio.

Los partidarios de la *Net Neutrality* temen que esta práctica se utilice para reducir la llamada 'apertura de la red'. Pero siendo justos, la DPI es sólo una tecnología y puede ser utilizada para cosas mejores (y peores) que infiltrarse en la comunicación de los usuarios de Internet para prohibir el uso de una determinada aplicación.

**Por ello, lo que hay que definir son los supuestos donde se pueden utilizar estas técnicas y hasta dónde pueden llegar.**

La *Net Neutrality* es un concepto a definir ya que se usa para referirse a cosas distintas, entre otras:

- La conexión punto a punto entre cualquier usuario de Internet.
- La gestión del tráfico en Internet, basada en sus distintos tipos, por parte de las operadoras.
- Las llamadas 'libertades en Internet' (enunciadas por la FCC<sup>3</sup>).
- El bloqueo de ciertas aplicaciones.

**Internet no es totalmente neutral hoy en día y esto hay que reconocerlo; los operadores gestionan tráfico. Por eso la clave no está en el 'qué' sino en el 'hasta dónde'.**

Las empresas que abogan por la *Net Neutrality* tampoco son inocentes ya que utilizan argumentos en favor del usuario como un medio para proteger un ecosistema que les es extremadamente favorable. Tratan de convertir a los usuarios en la punta de lanza de sus propias reivindicaciones. Plantean el debate como una lucha en la que las empresas de Internet y los usuarios se enfrentan a las operadoras. Una simplificación no del todo correcta.

Finalmente, hay que tener en cuenta que los usuarios son cada vez más inteligentes y están cada vez más conectados. Actual-

<sup>3</sup> <http://www.openinternet.gov/>

### Cuestiones sobre privacidad planteadas por el uso de *Deep Packet Inspection*

1. ¿Cuáles serían los usos apropiados de Deep Packet Inspection (DPI)?
2. ¿Cuándo debería ser usada la DPI y bajo qué autoridad?
3. ¿Qué procesos de gestión de la información deben ser usados por las organizaciones que practiquen DPI? ¿Terceras partes deberán poder tener acceso a dicha información?
4. ¿Cuáles deben ser los requerimientos en cuanto a la información facilitada al consumidor sobre el uso de DPI? ¿Cuáles deben ser las obligaciones de información en cuanto a las elecciones del consumidor sobre el uso de DPI para su seguridad? ¿Cuáles deben ser los requerimientos respecto del uso de DPI para la venta de información sobre perfiles de consumo a terceros?
5. ¿Qué información examinable bajo DPI sería personal y estaría sujeta a las leyes de privacidad?
6. ¿Debe concentrarse más atención en las decisiones sobre el diseño de Internet? La explotación de las debilidades de la arquitectura de Internet es una de las razones utilizadas para justificar la DPI.

Office of the Privacy Commissioner of Canada. <http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/>

mente existen mecanismos para la ‘encriptación’ del tráfico (*SSL encryption*) cada vez más sofisticados. Por lo tanto, la DPI sería una solución a corto plazo.

## Prácticas por parte de gobiernos: DPI y más allá

El debate sobre la DPI está amplificado por la gran controversia que existe actualmente por el control sobre Internet en la sociedad y los medios de comunicación. Efectivamente, el hecho de que Internet conforme una realidad paralela fuera del control de los gobiernos, empuja a éstos a buscar la forma de controlar su uso. Recientes situaciones en China, Irán, Emiratos Árabes Unidos y Rusia han alertado a la opinión pública mundial sobre intentos de control del uso que de Internet hacen los ciudadanos. Las prácticas pueden ir mas allá de la DPI y sus implicaciones pueden entrar de lleno en el terreno de las libertades individuales. El miedo a este tipo de prácticas afecta al debate que, con matices distintos, tiene lugar en sociedades democráticas.

En éstas también se usa la DPI. Por ejemplo, en Estados Unidos por cuestiones de seguridad nacional. En efecto, existe un acuerdo entre el Gobierno americano y AT&T para la vigilancia de las comunicaciones en Internet. El 50% del tráfico de la operadora pasa por los filtros del Gobierno.

## China

Desde la introducción de Internet en China en 1994, sus gobernantes han intentado conocer y controlar su uso por parte de la población.

En efecto, el Gobierno Chino vigila de cerca a los diferentes proveedores de acceso a Internet y a los ‘ciber-cafés’. Además, diversos sistemas de filtrado actúan en la arquitectura de Internet en China.

En la segunda mitad de los noventa, el sistema de censura pasó a ser conocido como ‘*Great Firewall of China*’ (un juego de palabras con la Gran Muralla china), porque se basaba en utilizar una tecnología de *router* para bloquear la información no deseada del exterior en el punto de entrada. Sin embargo, el uso de Internet ha crecido y esta herramienta se ha revelado como poco eficaz.

A finales de junio de 2009, el Gobierno chino anunció y posteriormente retiró una legislación según la cual se instalaba en todo ordenador un cortafuego en la navegación en Internet: el proyecto ‘Presa Verde’ (*Green Dam Youth Escort*). Aunque las autoridades manifestaron que su objetivo era evitar actividades como la pornografía infantil, diversas voces se manifestaron en la Red ante lo que se percibía como un nuevo intento de controlar Internet.

Desde el 1 de julio de 2009, cada PC vendido en China debía incluir un *software* de

filtrado de navegación en Internet. No quedaba claro si el *software* debía estar preinstalado en el ordenador o formar parte del sistema operativo para que fuese el usuario el que lo instalase.

Lo interesante de este caso era la constatación de la grandísima oposición por parte de los internautas chinos: *hackers* chinos lanzaron ‘ciberataques’ a la página web de los desarrolladores del programa<sup>4</sup>. Por otro lado, algunos fabricantes de equipos se mostraron reacios a incluir *software* no deseado por sus clientes.

Finalmente, como señalaba la revista *Economist* el 27 de junio de 2009, expertos de la Universidad de Michigan demostraron que este *software* podría dañar a los ordenadores; el programa estaba desfasado e incluía fallos de seguridad.

El Departamento de Comercio estadounidense presentó una queja frente al Gobierno Chino. Sin embargo, este último señaló que el objetivo de ‘*Green Dam*’ era proteger a la juventud de contenidos ‘poco sanos’. Los expertos de la Universidad de Michigan comprobaron que filtraba contenidos políticos.

## Irán

El Gobierno Iraní, a través de una subsidiaria del monopolio gubernamental iraní de las telecomunicaciones, compró un sistema para realizar *Deep Packet Inspection* en 2008 a una *joint venture* de Nokia y Siemens, llamado *Wavewasher*, se trata de un sistema de identificación y monitorización de Internet. Según informaba el *Wall Street Journal* en junio de 2009, el sistema permitía a las autoridades no sólo bloquear las comunicaciones, sino también monitorizarlas para conseguir información sobre individuos e incluso alterarlas.

La empresa justificaba la venta basándose en que el concepto de interceptación legal

de las comunicaciones está reconocido internacionalmente.

Aunque la empresa y sus competidoras han vendido sistemas similares a otros países, la diferencia entre ésta venta y otras, y el posterior escándalo, radica en el carácter de régimen iraní y en que estos instrumentos se han revelado como una herramienta de represión: el régimen iraní buscaba en los contactos de Facebook para identificar manifestantes.

A raíz de la venta del sistema de DPI para monitorizar y vigilar las comunicaciones en Internet, ciudadanos iraníes comenzaron una campaña de boicot a Nokia<sup>5</sup>. Las ventas de los terminales de la compañía, que lideraba hasta entonces en el mercado iraní, habrían caído en el país asiático.

Actualmente, Siria cuenta con 53 millones de usuarios de telefonía móvil, pero únicamente la clase media-alta utiliza *smartphones*. Las clases medias iraníes que han protagonizado la revuelta son los sectores sociales tecnológicamente más adelantados, los que utilizan Twitter en inglés.

Del mismo modo que se utiliza la Web para la movilización social, se utiliza también para lanzar iniciativas de boicot (en Facebook circula una lista de marcas iraníes a boicotear).

Finalmente, del mismo modo que Google ha sido muy criticada por transigir ante ciertas exigencias del Gobierno chino, Yahoo fue objeto de críticas por una supuesta colaboración con el gobierno Iraní durante el periodo post-electoral: habría suministrado información al Gobierno sobre sus usuarios a cambio de no ver bloqueados sus servicios.

## Rusia

Otra de las ideas para controlar Internet pasaría por crear partes de Internet más cerradas y a medida.

<sup>4</sup> Además, una empresa americana (Solid Oak Software) sostiene que el fabricante chino ha utilizado ilegalmente un código de su propiedad sujeto a *copyright*.

<sup>5</sup> <http://www.guardian.co.uk/world/2009/jul/14/nokia-boycott-iran-election-protests>

En octubre de 2009, el Icanm (la institución supervisora que organiza los nombres de dominio en Internet, entre otros aspectos) aprobó la decisión de permitir nombres de dominio que contuviesen caracteres no latinos. Una razón esgrimida por el Icanm es que la mitad de los 1.600 millones de usuarios de Internet hablan, como lengua materna, un idioma sin caracteres latinos.

A finales de 2009, Rusia desveló una iniciativa<sup>6</sup> para reivindicar el registro de dominios con caracteres cirílicos. La existencia de una parte de Internet con estos caracteres ha alertado a Internautas rusos, ya que con la imposición del alfabeto cirílico por la sociedad podría tener lugar una red y un uso en Rusia más cerrados al mundo exterior. Actualmente, las direcciones de dominio (2,5 millones en Rusia) y los correos electrónicos tienen caracteres latinos, mientras que sus contenidos pueden ser en caracteres cirílicos.

El éxito de esta iniciativa rusa prevista para el año que viene podría desencadenar iniciativas similares de China, Japón o de los países árabes.

Las autoridades rusas contestan que los miedos por una posible censura son infundados y que estas iniciativas no tienen por qué afectar a los contenidos. Por otro lado, afirman que Rusia no pretende instalar mecanismos de filtrado y *firewalls* en Internet como los de China.

## Emiratos Árabes Unidos

El verano pasado, los usuarios de Blackberry con el operador Etisalat, principal operador de telecomunicaciones de los Emiratos Árabes Unidos (cerca de 150.000 usuarios de Blackberry), recibieron un correo de la compañía para la actualización del *software* de su terminal. El argumento utilizado era la mejora en sus prestaciones. Sin embargo, la actualización bloqueaba el sistema operativo y reducía la batería del terminal. El servicio de atención al cliente de Etisalat, cuando

tuvieron lugar las primeras quejas, simplemente recomendó comprar baterías nuevas.

Research in Motion (RIM), la compañía fabricante de Blackberry, manifestó que no se trataba de una actualización oficial ni estaba autorizada. Lo que sería más preocupante es que RIM llegó a la conclusión de que el *software* distribuido estaba destinado a tareas de vigilancia y era capaz de acceder a informaciones privadas (correos, llamadas) del usuario.

No se trataba de un *software* que mejoraba la experiencia del usuario, sino de uno que enviaba mensajes sobre el usuario a los servidores centrales, desarrollado por una compañía norteamericana (SS8), que se presenta a sí misma como un proveedor de soluciones de vigilancia.

## Conclusión

La importancia de las prácticas de control del tráfico en Internet tiene implicaciones políticas y sociales muy importantes.

En este sentido, el debate alrededor del *Deep Packet Inspection* va más allá de lo que podría ser la gestión de la red para evitar su saturación, y se adentra en un debate más amplio sobre la privacidad y el uso que de la red hacen los individuos.

La gestión del tráfico en Internet por parte de los operadores es algo que existe y parece que va a seguir existiendo. Lo que se necesitan son reglas claras sobre quién estaría autorizado a realizar la gestión del tráfico y sobre dónde estarían los límites de dichas prácticas.

Esto es necesario porque una vez que los usuarios están alertados sobre ellas, han de saber para qué van a ser utilizadas.

El derecho a la privacidad del usuario parece una línea roja evidente: una cosa sería discriminar por el tipo de tráfico (video, P2P, etc.), otra discriminar por el contenido de ese tráfico.

<sup>6</sup> <http://www.nytimes.com/2009/12/22/world/europe/22cyrillic.html>

Para explicarlo de forma clara: una cosa sería discriminar el correo por su contenido, abriendo la carta; y otra, muy distinta, por el tipo y tamaño de paquete. Una cosa es discriminar el tráfico por ser P2P y otra discriminar por lo que se hace con esa tecnología.

La congestión de la red no obliga de manera necesaria a realizar estas prácticas, pero son posibles. Si hay congestión se debe aplicar un principio económico racional; si hay un recurso escaso, su precio debe subir. El que más descargue, que pague más por esa prioridad. Se trata de encontrar un precio justo basado en el volumen de tráfico. El acceso a toda la red puede ser garantizado, pero el volumen

de uso que se haga tendrá precios diferentes.

Es necesario que el usuario esté debidamente informado de las prácticas a las que se somete su tráfico, sin que esto afecte a su privacidad. Es necesario, también, que las mismas garantías jurídicas existan tanto en las comunicaciones físicas, como en las electrónicas.

La importancia de esto es también económica, ya que la innovación en la red y sus beneficios al resto de la economía necesitan unas reglas claras. Hasta ahora, Internet es una realidad abierta y descentralizada, y su desarrollo depende de esto.

ENTER