Intermediarios de internet. ¿La nueva policía informática?

Joe McNamee
European Digital Rights
www.edri.org

Introducción

El propósito de este informe es observar la creciente tendencia a usar a los intermediarios de internet como policía y brazo ejecutor de la ley e incluso para aplicar sanciones. Al mismo tiempo que lesiona los derechos fundamentales de libertad de comunicación, la privacidad y el derecho a un juicio justo, esta actitud sirve para crear limitaciones en el mundo en línea, socavando la apertura que le da a internet su valor para la democracia y, también, para la economía.

Este tema va creciendo en importancia debido a cuatro tendencias diferentes que se desarrollan en forma simultánea y sinérgica:

Las crecientes posibilidades técnicas de ejercer una vigilancia en línea con que cuentan las empresas proveedoras de acceso a internet. Algunas leyes tornan obligatorio el uso de algunas de estas posibilidades, como la Ley de comunicaciones de 2004 en Estados Unidos (Communications and Law Enforcement Act, CALEA)[1] y la Directiva de conservación de datos de la Unión Europea (UE)[2].

El creciente interés comercial que las proveedoras de acceso más grandes ven en bloquear o limitar ciertos contenidos en línea, como lo ilustran los recientes debates en Estados Unidos y Europa sobre la «neutralidad de la red».

La presión concertada en el nivel intergubernamental por legitimar y extender medidas de aplicación de la ley privatizadas[3].

Las fusiones de proveedoras de acceso y empresas de medios y los acuerdos de distribución entre proveedores de contenidos e intermediarios para adoptar medidas de vigilancia y punitivas[4].

Limitaciones de la responsabilidad intermediaria

Tanto Estados Unidos como la UE reconocieron la necesidad de una internet abierta a fines de los años 1990. Estados Unidos aprobó la Digital Millennium Copyright Act (Ley de derechos de reproducción para medios digitales, DMCA) en 1998, que ofrecía protecciones o amparos significativos a los intermediarios de internet por los contenidos no autorizados de sus redes, mientras que la UE emitió la Directiva de comercio electrónico en 2000, que adoptaba un tratamiento horizontal de los amparos ante toda forma de contenidos ilegales o no autorizados. Los objetivos de estas políticas públicas a ambos lados del Atlántico estaban claros: mantener una internet abierta. Esto se consideró necesario para que la economía pudiese aprovechar todas las ventajas de internet y, como beneficio secundario, la libertad de expresión y un acceso casi irrestricto a la información. Los beneficios de este tratamiento pueden verse en la economía[5] y en el papel de internet en la apertura de sociedades cerradas en todo el mundo.

1 en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act

2 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

3 Véase, por ejemplo, el artículo 5.3 del Acuerdo Comercial contra la Falsificación (ACTA) en trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147939.pdf

4 www.bof.nl/2011/01/04/vrije-internettoegang-ook-in-nederland-onder-vuur

5 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

Este informe forma parte del Monitor Mundial sobre la Sociedad de la Información 2011 sobre derechos en internet y democratización. Fue publicado originalmente en inglés por la Asociación para el Progreso de las Comunicaciones junto a Hivos con el apoyo de la Agencia Sueca Internacional de Cooperación al Desarrollo (Sida).
 giswatch.org/es/2011

Sin embargo, a pesar de este marco legal comparativamente sólido, las debilidades aparecieron casi desde el principio. Particularmente en Europa, donde la redacción de la Directiva de comercio electrónico es demasiado imprecisa (debido a los compromisos políticos durante el proceso de aprobación) como para que las empresas intermediarias se sientan completamente seguras, lo cual ha resultado en violaciones significativas del derecho a la comunicación. En 2004, un estudio de la ONG holandesa Bits of Freedom puso a prueba a doce proveedores de alojamiento web, nueve de los cuales borraron materiales inocentes como resultado una «notificación» visiblemente falsa enviada desde una cuenta de Hotmail abierta solo con ese propósito. La experiencia fue repetida en el Reino Unido por un grupo de académicos[6], también en 2004 (aunque debe señalarse que este proyecto halló que el procedimiento acorde a la DMCA era comparativamente sólido), y también por la empresa holandesa ICTRecht en 2009. Las empresas proveedoras de internet, en especial las que cambiaron sus actividades principales de ser proveedoras de alojamiento a proveedoras de acceso a internet, comenzaron a bloquear contenidos más allá de lo que indica la ley. Esto comenzó en el Reino Unido en 2004, con el apoyo de la Internet Watch Foundation, y se extendió a Dinamarca, Suecia y Finlandia en los años siguientes, como también al entorno móvil, gracias a un acuerdo intermediado por la Comisión Europea[7]. Vale la pena observar la coincidencia entre los actores del mercado de acceso a internet que más se oponen a la neutralidad de la red y los que apoyan el bloqueo voluntario.

Las operadoras que se ubicaron a la vanguardia del bloqueo «voluntario» de internet –como British Telecom, Telenor, Virgin y la industria de acceso móvil en general, son también las que más se oponen a la neutralidad de la red. En enero de 2011, British Telecom anunció planes para cobrarles más a ciertos proveedores de video en línea por tráfico priorizado[8], lo mismo hizo Telenor[9], mientras que Virgin Media anunció planes para lanzar una inspección profunda del tráfico de 40% de sus clientes en 2010[10]. De manera similar, sobran ejemplos de los esfuerzos de la industria de comunicaciones móviles por explotar y reforzar el control sobre sus clientes mediante, por ejemplo, el bloqueo de aplicaciones que siguen el protocolo VoIP[11]. Esto crea una situación en la que los proveedores están dispuestos a aceptar las demandas de los entes reguladores que exigen medidas de bloqueo «autorreguladas» ya que, en el largo plazo, les será difícil a los reguladores argumentar de manera creíble que los proveedores de acceso deben interferir voluntariamente en el tráfico por razones de política pública, pero no por razones comerciales.

El comienzo de la observancia privada

En este momento parecemos estar ante un «punto de inflexión», con gobiernos convencidos de que la apertura que le dio a internet su valor económico es tan inquebrantable que es posible fomentar la intromisión de las empresas intermediarias para la protección (principalmente) de la propiedad intelectual[12]. No solo propician esta postura internamente y en países con tradiciones democráticas fuertes, sino en todo el mundo, con la posibilidad de bloquear mercados y legitimar la vigilancia privada y el control de las comunicaciones en regímenes totalitarios y fuertemente controlados. Como resultado, se produjo una ola de medidas internacionales que buscan estimular u obligar a los intermediarios –muchas con sus propios intereses en esto– a filtrar, bloquear y sancionar las presuntas infracciones en línea.

En noviembre de 2010, las partes negociantes publicaron el texto final del Acuerdo Comercial contra la Falsificación (ACTA, por su sigla en inglés). Aunque mejor que las versiones anteriores, la sección que trata de los acuerdos sobre observancia de la propiedad intelectual se refiere, de manera elíptica, a la manutención de un régimen de responsabilidad de los proveedores de servicios de internet (PSI) que preserve «los intereses legítimos de los/as titulares de derechos» y obligue a las partes a «promover esfuerzos de cooperación dentro de la comunidad empresarial, para tratar de forma eficaz las infracciones de marcas de fábrica o de comercio y los derechos de autor o derechos conexos»[13] –una nota al pie en un borrador filtrado al público explicaba que «un ejemplo de esa política es disponer la cancelación, en circunstancias apropiadas, de las suscripciones y cuentas que los/as presuntos/as infractores/as posean en el sistema o red del proveedor de servicios».

6 pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

7 ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3153

8 www.wired.com/epicenter/2011/01/bt-rejects-accusations-of-net-neutrality-breach-sort-of

9 www.dn.no/forsiden/etterBors/article2067200.ece

10 technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6989510.ece

11 www.ft.com/cms/s/0/1ce4e1c8-1fd7-11de-a1df-00144feabdc0.html#axzz1STK17d9n

12 Un grupo de 108 profesores universitarios denunció en una carta pública que el proyecto de ley PROTECT IP de Estados Unidos permite que «el gobierno viole el sistema de direcciones de internet» y «viole la infraestructura de internet». blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf

13 trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147939.pdf

En febrero de 2011, la Organización Mundial de la Propiedad Intelectual (OMPI) intentó[14] lanzar una discusión[15] sobre la responsabilidad de los intermediarios en la violación de marcas comerciales, pero fracasó. A esto le siguió un evento paralelo durante una reunión de OMPI en Ginebra, en junio de 2011, sobre «el rol y responsabilidad de los intermediarios de internet en el campo de los derechos de autor», ique no incluyó a ningún intermediario de internet! OMPI también publicó recientemente dos estudios independientes sobre la responsabilidad de los intermediarios[16]. Logró llevar adelante una propuesta de taller al Foro de Gobernanza de Internet en Nairobi, en septiembre de 2011, para debatir ideas y reflexiones, como las que se encuentran en ACTA, la Ley de infracciones y fraudes en línea de Estados Unidos (COICA, en inglés) (que les exige «bloquear» a los intermediarios) y la Directiva de la UE relativa al respeto de los derechos de propiedad intelectual (cuyas disposiciones sobre vigilancia y bloqueo de internet están bajo revisión del Tribunal de Justicia de la UE)[17].

En junio de 2011, la Organización para la Cooperación y el Desarrollo Económico (OCDE) adoptó su Comunicado sobre los principios para la elaboración de las políticas de internet[18]. Bajo el título «limitación de la responsabilidad civil de los intermediarios de internet» llama a los estados a convocar a un proceso multipartito para «determinar bajo qué circunstancias los intermediarios de internet podrían dar pasos para educar a los/as internautas, asistir a los titulares de derechos para hacerlos valer o reducir los contenidos ilegales» (el comunicado en sí fue tema de un proceso multipartito que la sociedad civil rechazó)[19]. El texto evita apoyar la neutralidad de la red y en su lugar se refiere, sin demasiado objeto, a mantener una calidad «apropiada». También evita toda referencia al debido proceso, utilizando «proceso justo», una expresión menos restrictiva pero que no tiene valor legal.

La vigilancia privatizada en la práctica

¿Qué significa todo esto en un nivel práctico? Como este abordaje no está regido por una ley, la implementación suele ser muy ad hoc. En Europa, proveedores de alojamiento en internet y redes sociales suprimen materiales que suponen podrían acarrearles demandas de responsabilidad civil, apoyándose en criterios bastante azarosos. Como mostró el estudio realizado en 2004 por Bits of Freedom, un mismo contenido puede ser suprimido o permitido según las impredecibles prácticas internas de las empresas en cuestión. La red social holandesa Hyves borrará algo automáticamente si usuarios y usuarias con diez direcciones IP diferentes pulsan el botón «denunciar este material». Por su parte, la Comisión Europea alienta activamente a proveedores de alojamiento a cambiar sus condiciones de servicio para adjudicarles capacidad irrestricta de suprimir cualquier cosa que deseen[20]. De manera similar, a las proveedoras de internet que comenzaron a «bloquear» sitios web acusados de contener materiales de abuso de menores, se les solicita ahora –y a veces se les exige– que introduzcan medidas para bloquear otros contenidos.

En Irlanda, la anterior proveedora monopólica de internet Eircom acordó convertirse en juez, jurado y ejecutor de acusaciones de descarga ilegal, incomunicando a consumidores y consumidoras con acusaciones de infracciones reiteradas[21] y bloqueando sitios web[22] que los intereses de la industria musical acusan de facilitar infracciones. La ley española conocida como «Sinde» muestra una interesante mezcla de principios legales y coerción extrajudicial. Bajo esta norma, un/a fiscal exige primero medidas extrajudiciales de parte del proveedor de internet y luego, si éste quiere incurrir en los gastos que conlleva llevar el caso a tribunales, se abre un proceso judicial. En Estados Unidos, las grandes ISP que presionan duramente por el derecho a regular el ancho de banda para su propio beneficio comercial ofrecen magnánimamente estrangular el ancho de banda de usuarios y usuarias que posean acusaciones reiteradas de infringir la propiedad intelectual.

Además de los intereses comerciales que anidan en esta posición contraria a la neutralidad de la red, la naturaleza cambiante del negocio (demostrada entre otras cosas por la compra de NBC por Comcast y el reciente movimiento de Verizon hacia la distribución de películas)[23] crea nuevos incentivos para esta actitud. Las proveedoras de acceso más pequeñas se encontrarán cada vez más restringidas –están obligadas a cubrir los costos de implementación de tecnologías capaces de

14 www.ccianet.org/index.asp%3Fsid=5%26artid=213%26evtflg=False
15 www.wipo.int/edocs/mdocs/sct/es/sct_25/sct_25_3.pdf
16 www.wipo.int/copyright/en/internet_intermediaries/index.html
17 Tribunal de Justicia de la Unión Europea, Caso C70/10.
18 www.oecd.org/dataoecd/40/21/48289796.pdf
19 www.edri.org/files/CSISAC_Press_Release%20_0628011_FINAL.pdf
20 www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-comission
21 www.theregister.co.uk/2009/02/03/eircom_agrees_to_three_strikes_enforcement
22 www.theregister.co.uk/2009/02/23/irma_demands_irish_isps_block_access_to_piracy_sites
23 www.nytimes.com/2011/07/17/opinion/sunday/17sun3.html?partner=rssnyt&emc=rss

interferir el tráfico de internet en ausencia de una economía de escala que les permitiría hacerlo en forma económicamente eficiente o en forma que podría usarse para propósitos contrarios a la neutralidad de la red.

A las amenazas a la capacidad de la ciudadanía de acceder a internet, o de acceder a una internet abierta y neutral, y acceder a material «voluntaria» o accidentalmente bloqueado por su PSI, se suman esfuerzos crecientes por usar la misma estructura de internet como herramienta de imposición de la ley. La UE y Estados Unidos, por ejemplo, tienen entre manos un proyecto para debatir la revocación de nombres de dominio (sobre los cuales Estados Unidos reclama una amplia jurisdicción)[24] y direcciones IP[25] (el registro regional de Europa, Oriente Medio y partes de Asia central se ubica en Holanda). Mientras que la posición de Estados Unidos se basa parcialmente en un marco legal, con las leyes COICA y PROTECT IP (ley de prevención de amenazas en línea a la creatividad económica y robo de propiedad intelectual)[26] que prevén regular el bloqueo y revocación de nombres de dominio, también adopta una posición no legislativa en algunas circunstancias, como las farmacias no autorizadas en línea. En algunos países de la UE (Francia e Italia, por ejemplo), el bloqueo está regulado por ley; en otros (Reino Unido y Suecia) se lleva adelante sin ley, y aún en otros se aplica con o sin ley, según el asunto (como en Dinamarca y posiblemente en el Reino Unido en un futuro próximo). La revocación de nombres de dominio, por otra parte, no tiene marco legal[27].

Conclusión

La promoción de una internet cerrada y regulada por fuera de un marco legal socava los esfuerzos de los gobiernos occidentales por apoyar el potencial democratizador de internet en regímenes cerrados y totalitarios. La imposición de reclamos de jurisdicción poco razonables sobre partes o todos los sistemas de asignación de direcciones IP y nombres de dominio genera un peligro para la integridad de internet en todo el mundo. La tercerización de la vigilancia en internet y la imposición de sanciones por intermediarios de internet contradicen valores democráticos básicos y la noción de vigencia de la ley en nuestras sociedades democráticas. La tercerización de estas actividades a grandes corporaciones que tienen fuertes intereses, admitidos públicamente, en el desarrollo e imposición de una red no neutral crea un entorno en línea diametralmente opuesto a la apertura de internet. Esta apertura es la que provee el valor democrático –y económico– de internet y es demasiado importante como para que los gobiernos la den por sentada y experimenten con ella como si fuera insignificante. De manera creciente, nuestra interacción social se produce en línea y las libertades que antes nadie cuestionaba pueden quedar ahora al arbitrio de empresas privadas: nuestra libertad de expresión, nuestra libertad de reunión, nuestra privacidad y nuestro derecho al debido proceso y a la presunción de inocencia.

Próximos pasos

Los y las activistas deberían exigir que se respeten el espíritu y la letra de los derechos constitucionales[28] y los derechos humanos[29].

Deberían reconocerse los peligros de forzar a regiones del mundo o países individuales a desarrollar «splinternets» (escisiones de internet) para evitar la jurisdicción de Estados Unidos y la UE.

Las posiciones positivas de las organizaciones internacionales deben recibir la mayor publicidad posible[30].

Las declaraciones positivas sobre la necesidad de mantener la apertura de internet deberían recibir publicidad y promoción[31].

Deben destacarse las contradicciones entre los llamados a la apertura de internet en ciertos países y el apoyo a una red cerrada y con regulación privada en el ámbito nacional.

Debería prestarse más atención a los perjuicios económicos de pasar de una internet innovadora, competitiva y abierta a una internet cerrada y no neutral. ■

24 digitizor.com/2011/07/06/us-jurisdiction-com-net-websites

25 www.theregister.co.uk/2010/04/27/eu_cybercrime

26 en.wikipedia.org/wiki/Protect_IP_Act

27 www.theregister.co.uk/2011/05/18/nominet_wrestles_with_net_cop_role

28 Como la primera enmienda de Estados Unidos.

29 Como los artículos 8 y 10 de la Convención Europea de Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.

30 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

31 www.physorg.com/news/2011-02-clinton-renews-internet-access.html