

## Una aproximación al debate sobre la gobernanza de Internet (Cuarta parte)

### ¿Seguridad versus privacidad?

*\*Por Alexandra Dans.*

Como los problemas de seguridad tienen consecuencias de índole económica, social y política e influyen los debates tanto sobre la privacidad como sobre la libertad de expresión, se ha destacado en varios foros internacionales la dificultad de encontrarles una solución viable a corto plazo. Como en todos los temas que atañen a Internet, las causas de dichos problemas son múltiples y existen incontables actores involucrados.



**Caricatura de Kichka**

Desde las primaveras árabes, se ha hablado principalmente del uso de Internet tanto por activistas como por los regímenes que buscaron reprimirlos (por ejemplo, al espiar la actividad en la red de los militantes o al bloquearles el acceso a Internet). Según Amnistía Internacional, el uso activista de Internet es un arma a doble filo y “en China, donde las autoridades temen un contagio de la “primavera árabe”, el control de internet, que ya era estrecho, fue reforzado.” (1) En ese país, han incluso desaparecido varios activistas internautas desde que se llamó vía Internet a la población a sublevarse en febrero de este año para la “revolución del jazmín” (*jazmin revolution*) (2)

Muchas acciones realizadas por Hackers, como los integrantes del grupo Anonymous (3), han sido decisivas en el triunfo de las revoluciones de Túnez y Egipto. El grupo hoy apoya abiertamente el movimiento ciudadano español [15M](#) y más globalmente, al movimiento “Occupy” que se inició en [Wall](#)

[Street](#) en septiembre de este año y que ahora cuenta con diferentes apoyos en todas partes del mundo, implementándose ocupaciones en varios países a nivel global. Ha nacido el concepto de “hacktivism”.

Si se considera el problema desde un punto de vista político, el tema de la Seguridad en Internet tiene entonces dos caras:

- Por un lado, encontramos los que representan a los gobiernos que quieren monitorear y controlar la información que comparten y publican sus ciudadanos en Internet para proteger el statu quo, mantenerse en el poder y promover su agenda política;
- Por otro lado, los que quieren que sus voces sean oídas y que cuentan con apoyo alrededor del mundo, que hackean los sitios web en desacuerdo con sus creencias o ideales políticos. (4)

Uno de los puntos discutidos durante la sesión “El futuro de la Privacidad” (*The Future of Privacy*) en el Quinto Foro de Gobernanza de Internet realizado en Vilnius, Lituania (Septiembre 2010) hacía justamente referencia a la necesidad de incluir una protección vis-à-vis de los gobiernos y especialmente garantías jurídicas contra el acceso del gobierno a las comunicaciones privadas de sus ciudadanos. (5)

Pero los problemas de seguridad y de privacidad en Internet son aún más complejos y no suponen únicamente causas y consecuencias de índole política. También existen las de orden social (por ejemplo, la existencia de contenido considerado ofensivo) y económico (por ejemplo, los problemas de *spam*, *address spoofing*, usurpación de identidad, etc.). La dificultad reside en el anonimato permitido por la Red y en el hecho que el intento por parte de algunos gobiernos de implementar medidas ya sea para rastrear transacciones electrónicas o censurar información han sido “muy mal recibidas por los usuarios de Internet que ven estas medidas contrarias a la libertad de expresión, y por los operadores económicos en general, pues consideran que se trata de restricciones innecesarias que perjudican el desarrollo de Internet y del comercio electrónico”. (6)

Planteado este claro conflicto de intereses, el problema parece no tener solución. La implementación de legislaciones o normativas para “controlar” el uso de Internet con el propósito de “proteger” a los usuarios es considerado por estos últimos como una invasión a su privacidad y un atropello a sus derechos.

¿Hasta qué punto es positivo el registro y la monitorización de nuestras huellas digitales para la protección del ciudadano común y especialmente de nuestros niños (por ejemplo para poder contrarrestar y eliminar páginas de pornografía infantil)? ¿Cómo asegurarnos de que ese rastreo no tiene otros fines (comerciales o políticos) o no podrá servir otros propósitos en el futuro? ¿Este tipo de acción de “protección” de los ciudadanos debe recaer en manos de gobiernos, de la comunidad global, de grupos como Anonymous (7)?

¿Debe primar la seguridad sobre cualquier otra consideración? ¿Cómo entonces considerar las acciones de grupos como Wikileaks (8) que algunos consideran

como una grave amenaza para la seguridad en tanto otros lo ven como una interesante oportunidad de empoderamiento ciudadano a través de la transparencia que permite?

Nos esperan desafíos varios si lo que se pretende es contrarrestar las amenazas múltiples expuestas brevemente en esta nota. Las cuestiones de seguridad y privacidad parecen ser los grandes temas constantes de debate sobre el Internet presente y futuro. Aún no parecen acercarse tiempos de uso libre y sin miedo de Internet.

(1) "Internet, un arma de doble filo para la "primavera árabe", según Amnistía Internacional": <http://informe21.com/facebook/internet-arma-doble-filo-primavera-arabe-segun-ammistia-internacional>(Informe21.com, mayo 2011)

(2) "Chinese activists disappear amid calls for protests": [http://www.usatoday.com/news/world/2011-03-03-china04\\_ST\\_N.htm](http://www.usatoday.com/news/world/2011-03-03-china04_ST_N.htm) (USA Today, marzo 2011)

(3) Anonymous es un grupo internacional de ciberactivistas que nació en el año 2003 a favor de la transparencia, de la libertad de expresión y de la independencia de Internet. Sus miembros son anónimos y en demostraciones públicas, suelen usar la máscara del protagonista de la película *V de Vendetta* para esconder sus rostros.

(4) Kovacich, Gerald, "What caused the Internet Security Problems?", *Computer, Fraud and Security*, Volume 2000, Number 4, 1 April 2000, pg 12.

(5) United Nations, *Developing the future together, The Fifth Internet Governance Forum* (Vilnius, Lithuania), UNON, 2011, pg 201.

(6) Pérez, Jorge (Coordinador), *La gobernanza de Internet, contribución al debate mundial sobre la gestión y el control de la red*, Fundación Telefónica, 2008, pg 80.

(7) Al momento de escribir esta nota, el grupo Anonymous atacó una importante red de pornografía infantil (unos 40 sitios web) y publicó una lista con los nombres de los usuarios de dichos sitios (más de 1.500 nombres) a través de lo que llamaron la "operación DarkNet".  
*Anonymous Hackers Take Down Child Porn Websites, Leak Users' Names*:  
<http://www.securitynewsdaily.com/anonymous-hackers-child-porn-sites-1260/> (Security News Daily, 20 de octubre 2011).

(8) "WikiLeaks (del inglés *leak*, 'fuga', 'goteo', 'filtración [de información]') es una organización mediática internacional sin ánimo de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes. El lanzamiento del sitio se realizó en diciembre de 2006, su actividad comenzó en julio de 2007 y desde entonces su base de datos ha crecido constantemente hasta acumular 1,2 millones de documentos. Su creador fue Julian Assange". Wikipedia: <http://es.wikipedia.org/wiki/WikiLeaks>

*\*Master en comunicación internacional de la Universidad de Québec en Montreal, se desempeña como coordinadora de cooperación internacional en el Registro regional de direcciones de Internet para América Latina y Caribe - LACNIC*

Además vea la primera entrega [aquí](#) y la segunda entrega [aquí](#) y la tercera entrega [aquí](#)