

Nueva Sociedad Separatas

Rodrigo Araya Dujisin
El factor sociotecnológico

Artículo aparecido en Nueva Sociedad 177, enero-febrero 2002, pp
154-160.

El factor sociotecnológico

Los atentados de septiembre de 2001 se produjeron cuando las protestas antiglobalización estaban en su apogeo. Las nuevas medidas de control sobre la privacidad en internet vienen a justificar las censuras impuestas desde hace tiempo por los Estados con políticas restrictivas sobre el tema.

Rodrigo Araya Dujisin

Sabemos que internet es una herramienta para la acción colectiva, aumenta las capacidades operativas de individuos, grupos, redes y movimientos sociales. Sabemos además que las plataformas electrónicas configuran nuevas formas de organización y asociatividad, favorece el reclutamiento de apoyos y la difusión de las ideas. Sabemos también que permite establecer vínculos con los procesos globales, interconectando conflictos y adversarios locales. El movimiento antiglobalización es un claro ejemplo de ello. Agrupa desde defensores de los animales hasta activistas por los derechos humanos, pasando por intelectuales, campesinos sin tierra y quienes se oponen a la manipulación genética de los alimentos. Múltiples causas y conflictos locales se interconectan, se coordinan y se potencian en escenarios globales.

La urgencia por fijar marcos de comprensión para el ataque a los centros simbólicos del poder financiero y militar por parte de redes fundamentalistas islámicas llevó a algunos a establecer apresuradas equivalencias entre los ataques metafóricos a los McDonald's y los ataques terroristas a las torres gemelas y el Pentágono. Según sabemos la «puesta en escena» en el McDonald's de Millau¹ consistió en llenar el local de animales y verduras en protesta por sanciones comerciales impuestas por Estados Unidos que afectaban a los productores de queso de cabra. En Seattle se realizaron marchas alegóricas, en Davos hace un par de años los ecologistas hicieron una espectacular aparición con

Rodrigo Araya Dujisin: investigador de Flacso-Chile.

Nota: Agradezco los comentarios de Florencio Ceballos y Claudio Rutllant de Ekhos I+C y Carlos Osorio de la Universidad de Harvard.

Palabras clave: globalización, internet, acción colectiva, control político.

paracaídas de colores en la reunión del Foro Económico Mundial, a la que no estaban invitados.

Algunos improvisados analistas, cuyas únicas fuentes parecen ser las cadenas globales de TV, han señalado con soltura que hay grupos antiglobalización blandos y duros y, sobre ese marco, han establecido múltiples vínculos entre un fenómeno y el otro. Esto equivale a decir algo así como que el señor que me vende el diario y Bill Gates son empresarios, que una lágrima es igualmente agua como el Pacífico. Claramente este tipo de análisis no nos ayuda mucho. Agregaría que las diferencias no solo pasan por un asunto de escala, sino de naturaleza del conflicto. La asimilación conduciría a criminalizar y a silenciar un debate que es político y se refiere a los contenidos de la globalización.

*internet
da para todo
y en muchos
aspectos es
un espejo
de la sociedad*

No está de más señalar que un acto terrorista, por definición, enfatiza el componente psicológico y que la moral civil se vuelve un objetivo militar, mientras que los activistas globales expresan valores internacionalistas y la convicción de que la democracia global debe ser un contrapeso a la mundialización financiera. Por lo demás, Atacc² y otros grupos antiglobalización han hecho tempranas declaraciones (no reproducidas en las cadenas de TV) de rechazo a las acciones terroristas. En Roma, Berlusconi organizó una manifestación de solidaridad con EEUU que congregó a 40.000 personas, con artistas muy conocidos y gran cobertura de prensa. El mismo día se realizó una manifestación por la paz, convocada por las redes antiglobalización movilizadas en Génova en julio de 2001, a la que asistieron 100.000 personas.

Las distintas redes han alertado sobre la asimilación que los quiere presentar como equivalentes a los terroristas. Sin embargo, la radicalidad de este movimiento se da en el plano de las ideas y su arma es la protesta.

La catarsis colectiva en internet

Lo cierto es que internet da para todo y en muchos aspectos es un espejo de la sociedad. En internet caben todos. Esta afirmación no responde a un decreto, es

1. Pequeña ciudad francesa donde se produce el queso roquefort.

2. «Asociación por una tasa a las transacciones financieras en ayuda a los ciudadanos», es un movimiento internacional para el control democrático de los mercados financieros y de sus instituciones. Es una de las principales redes de convergencia de las resistencias a la globalización.

parte de su arquitectura tecnológica y de lo que sus usuarios han hecho de la red, apropiándose de ésta para sus fines particulares y, por lo mismo, inyectándole vitalidad más allá de los anhelos o expectativas de reguladores o analistas. Es así como poco después de los atentados terroristas en EEUU, un grupo de jóvenes musulmanes estadounidenses puso en marcha un sitio en internet denominado «Musulmanes contra el terrorismo» (www.muslimsagainstterrorism.org) con el objetivo de honrar a las víctimas y defender la imagen del islam. Igualmente ha sucedido con los simpatizantes de Osama Bin Laden, quienes organizados en listas de discusión, sitios y *chats* comparten sus puntos de vista. Otros se van a los puños virtuales. En estos días un grupo de *hackers* informáticos violó un sitio de la compañía Trade Winds Communications y dejó una amenaza para Microsoft y un llamado a la utilización del sistema operativo Linux³, insultos contra EEUU e Israel y alabanzas para Bin Laden. La pantalla puede ser un campo de batalla. *Hackers* israelitas han destruido el sitio de Hezbolá y éstos el sitio del parlamento israelí. Algo similar ocurrió con el sitio del Departamento de Estado norteamericano, que fue violado por expertos chinos durante el incidente del avión espía, o escaramuzas electrónicas entre prochechenos y rusos.

Por otro lado, en Chile tras los atentados en EEUU, la búsqueda de familiares y amigos se realizó fundamentalmente a través de un portal para la comunidad de chilenos residentes en el extranjero. El portal casachile.cl con la Cruz Roja implementó horas después de los ataques un sistema de acopio de información y contactos para la ubicación de personas de paradero desconocido. Asimismo la comunidad académica en internet ha producido una cantidad impresionante de reflexiones y centros de recursos para comprender el episodio, expresar sentimientos de desconcierto, de odio o de temor, condolencias, cartas abiertas, etc. En listas de interés en las que participo se ha visto cierto desconcierto por el aumento explosivo de mensajes, y en varias ha sido imperioso crear listas paralelas para dar cabida a la necesidad de comunicación y expresión que provocaron los atentados.

El dilema de fondo: libertad o privacidad

Desde el 11 de septiembre de 2001 varios países han promulgado rápidamente nuevas leyes que buscan reforzar la vigilancia en internet. Con los poderes que

3. Linux es un equivalente a Windows que simboliza las causas libertarias en internet. Es un programa de código abierto y quien lo modifica lo devuelve a la comunidad de programadores y usuarios, para todos y gratuitamente. Hoy en día tiene 30 millones de usuarios.



le otorga la nueva ley antiterrorista, en EEUU el FBI podría reorganizar la arquitectura de internet. La organización Privacidad Internacional (PI) señala en su sitio que la ley amplía el uso de las escuchas telefónicas y del sistema de rastreo electrónico Carnívoro, y que convierte a los *hackers* en ciberterroristas. Carnívoro estaría instalado en los proveedores de internet (ISP) para permitir al FBI hacer seguimiento a las comunicaciones vía internet. Carnívoro, al igual que Echelon, son sistemas de espionaje que interceptan las comunicaciones privadas. Siempre se dijo que eran fantasías de informáticos y que no existían tales sistemas. La comisión parlamentaria europea creada en junio de 2000 para investigar esa red aprobó en Estrasburgo, días antes de los atentados, un informe

que confirma la existencia de Echelon. La Eurocámara sugiere en el informe que los ciudadanos codifiquen su correo electrónico.

La Fundación Frontera Electrónica ha condenado la legislación por la rapidez con que se ha aprobado, atropellando las libertades civiles. El presidente Bush ha solicitado a la Unión Europea que también revise sus normas sobre protección de datos. Algunas empresas de internet, en tanto, planean trasladar sus servidores desde EEUU hacia sus propios países. En internet se está produciendo un agudo conflicto entre la libertad individual y la seguridad. Las organizaciones que defienden las libertades individuales se han manifestado en varios países contra estas medidas. Algunos se esfuerzan en recordar convenciones y acuerdos internacionales de derechos humanos que prohíben toda forma de vigilancia electrónica general y que resguardan la libertad de información y expresión.

Dentro de los códigos consuetudinarios de la red se destaca su carácter igualitario⁴, en el sentido de que pueden traspasarse diferencias de clase, generacionales o de diversa índole. El otro principio apela a que la información en internet es esencialmente libre. Sin embargo, gobiernos y empresas han buscado la seguridad mediante la regulación y la capacidad represiva de las instituciones más que a través de la autoprotección tecnológica de los ciudadanos. De allí la importancia de la encriptación, que consiste en la codificación del lenguaje mediante claves secretas conocidas solo por el emisor y el destinatario del mensaje. Las tecnologías de encriptación hacen muy difícil la interceptación de los códigos de acceso y el contenido de la comunicación, y es uno de los aspectos centrales en la discusión tecnológico-social para la preservación de la libertad en internet. Tanta importancia se atribuyó a esta tecnología que se la clasificó en el rubro de armamento de exportación prohibida sin un permiso especial del Departamento de Defensa. La encriptación representa la posible autonomía para los individuos y organizaciones de cualquier índole con respecto a los gobiernos y a las grandes empresas. Phil Zimmerman, un matemático experto en tecnologías de encriptación difundió en 1991 en internet su sistema Pretty Good Privacy (PGP), en respuesta a los intentos del Senado estadounidense de prohi-

4. No está de más decir que internet nació y se ha desarrollado como una tecnología abierta y sus fundamentos y prácticas refieren a dos principios: igualdad y libertad. Igualdad y libertad para la minoría que tiene acceso. Para este año se estima que 4% de la población mundial cuenta con acceso a internet, con una disparidad entre países abismante. En los países desarrollados el porcentaje de conectados llega a 50%. En Nueva York hay más huéspedes (computadores que alojan sitios) que en toda África, y en Finlandia más que en toda América Latina y el Caribe; 40% de la población mundial no tiene acceso a luz y 60% no ha realizado jamás un llamado telefónico.

bir la encriptación en el marco de la legislación antiterrorista. Zimmerman sufrió persecución judicial, pues la publicación en internet supuso que, desde el punto de vista jurídico, equivalía a exportar armamento sin licencia.

Los más pesimistas auguran el comienzo de un periodo de caza de brujas en la red, haciendo peligrar gravemente el derecho a la privacidad. John Naughton, de la Universidad de Cambridge y columnista del *The Observer* de Gran Bretaña, dijo recientemente en una entrevista que en un sentido los terroristas ya ganaron y lo que nos espera es un futuro orwelliano. No son pocos quienes sostienen que el dilema entre libertad y control se terminó el 11 de septiembre. En nombre de la seguridad se aplicarán férreos controles a derechos a la intimidad de los correos electrónicos y de los foros, listas y contenidos de la red.

¿Quiénes le temen a internet?

Hay quienes consideran a internet como un enemigo en sí mismo. El gobierno talibán lo prohibió días después de los atentados y la represalia estadounidense, pero no ha sido el único. Según un reciente estudio de Reporteros sin Fronteras, existen cerca de 40 países que presentan fuertes restricciones a internet, que van desde el control estatal al acceso y contenidos hasta la prohibición total. Dentro de los argumentos que respaldan estas medidas se señala que se protege a la población de ideas subversivas para garantizar la seguridad y unidad nacional. Algunos países sustentan las prohibiciones estrictamente por razones culturales o religiosas, otros por razones políticas. En casi todos los casos los ciudadanos privilegiados con acceso a la red encuentran medios para eludir la censura. Los casos más graves de censura y prohibición son Arabia Saudita, Azerbaiyán, Bielorrusia, China, Corea del Norte, Cuba, Irak, Irán, Kasajistán, Kirguistán, Libia, Myanmar, Sierra Leona, Siria, Sudán, Tayikistán, Túnez, Turkmenistán, Uzbekistán y Vietnam.

Para los países islámicos como Arabia Saudita e Irán, se prohíben sitios que proporcionen información contraria a los valores islámicos, aunque en general se considera a internet como un factor de occidentalización de las mentalidades. En China y Cuba no se prohíbe internet, pero existe un fuerte control estatal en el acceso a la red y en los contenidos posibles de visitar. En 1999, en Shangai se encarceló a Lin Hai por proporcionar las direcciones de correo electrónico de 30.000 internautas chinos a una revista electrónica disidente publicada en un sitio cuyo servidor reside en EEUU. Asimismo en fecha cercana al décimo aniversario de la matanza de Tiananmen, se clausuraron 300 cibercafés en Shangai. Hay países donde no existe acceso a internet. Es el caso de Corea

del Norte, Irak y Libia. En Siria solo tienen acceso las instituciones oficiales y en Vietnam hay que pedir una autorización.

En estos casos, incluyendo las últimas medidas norteamericanas, los fines que justifican las restricciones al acceso y diseminación de contenidos son razones de Estado (lucha contra el terrorismo, narcotráfico, preservación de los valores e identidades, de la seguridad interior, amenazas externas, etc.) y todos ellos comparten una simetría notable: «Nosotros, el Estado, debemos saber lo que usted lee y escribe y con quien se comunica, para protegerlo mejor», y en todos estos casos los perjudicados son los propios ciudadanos y los disidentes, pues han sido puestos bajo una sospecha general, solo porque ahora el Estado puede usar tecnología que aumenta su capacidad para influir.

Resulta preocupante que la capacidad técnica de estas medidas sea tremendamente efectiva contra las personas y ONGs, contra los disidentes e inconformes que utilizan la red como simples usuarios o ciudadanos, que contra aquellos grupos terroristas o narcotraficantes que emplean formas de comunicación y de coordinación operativa mucho más sofisticadas, como lo

demuestran los atentados del 11 de septiembre. Peor aún, los Estados que tradicionalmente reprimen las libertades de expresión ahora tendrán una justificación política, siguiendo las medidas de EEUU, para «combatir el terrorismo» (y de paso la disidencia), y dispondrán de una floreciente industria de control y vigilancia electrónicos para satisfacer las necesidades de seguridad.

