Periodística [Societat Catalana de Comunicació], número 17 (2016-2017), p. 85-103
http://revistes.iec.cat/index.php/periodistica / DOI: 10.2436/20.3008.02.44
ISSN (ed.impresa): 1130-183X / ISSN (ed. electrònica): 2013-9985
Data recepció: 28/02/14 / Data acceptació: 20/12/14

Sabotajes virtuales y bloqueos informáticos como estrategias para las dinámicas de acción y la libertad de información

Noelia García Estévez

Resumen

En el entorno digital se fomentan imaginarios colectivos, identidades y conflictos sociales, a la vez que se articulan nuevas vías de acción y de actuación ciudadana. De este modo, en los últimos años se han desarrollado una serie de movimientos gestados desde la red y con un importante componente tecnológico. En este ciberactivismo encontramos una vertiente más radical en la que la figura del *hacker* se alza como un combatiente del cibercontrol y de las injusticias sociales. El objetivo de este artículo es analizar el desarrollo y la situación actual de estas acciones hacktivistas que utilizan técnicas como los ataques tecnológicos o los virus informáticos a favor de determinadas protestas sociopolíticas y de la extensión de la libertad de información. Los movimientos como Anonymous, LulzSec o WikiLeaks ponen de manifiesto el auge de este tipo de organizaciones no exentas de polémica y provocan una fuerte escisión entre sus defensores y sus detractores.

PALABRAS CLAVE: ataques tecnológicos, virus informáticos, hackerismo, libertad de información, activismo.

Virtual sabotage and computer blockades as strategies for action dynamics and freedom of information

Abstract

In the digital environment, collective imaginaries, identities and social conflicts are promoted. At the same time, new avenues of action and citizen participation are

implemented. This has led in recent years to the development of a series of movements which arose on the Internet, all of which have a significant technological component. This cyberactivism shows a more radical aspect in which the hacker stands as a fighter against cybercontrol and social injustice. The purpose of this paper is to analyse the development and the current state of the hacktivist actions that use such techniques as technological attacks or computer viruses for socio-political protests and the promotion of freedom of information. Movements such as Anonymous, LulzSec or WikiLeaks show the upswing of this type of organizations, which are not without controversy and which are producing a major split between their supporters and detractors.

KEYWORDS: technological attacks, computer viruses, hackerism, freedom of information, activism.

Introducción

Desde hace unos años vivimos insertos en una era tecnológica en la que tiene lugar una revolución digital capaz de modificar conceptos y actitudes. De hecho, nuestra sociedad ha experimentado un importante giro en el propio desarrollo de la ciudadanía, sus hábitos, costumbres y maneras de proceder. La inclusión de una esfera digital predominante y el imparable desarrollo tecnológico han propiciado un nuevo contexto en el que es preciso reformular las significaciones tradicionales, los imaginarios sociales y las actividades cívicas. Recordemos la tesis de Echeverría según la cual existen tres entornos de la humanidad: el entorno primero o *physis*, el entorno segundo o *polis* y el entorno tercero o *telépolis*. El primer entorno se refiere a todo aquello que es natural, el segundo trata del espacio social y cultural y el tercero hace referencia a un escenario «que difiere profundamente de los entornos naturales y urbanos en los que tradicionalmente han vivido y actuado los seres humanos» (Echeverría, 1999: 14). Se refiere a un entorno articulado a través de las tecnologías de la información y la comunicación y en el que se han visto sustancialmente modificadas las relaciones sociales y culturales que se dan y se daban en los entornos primero y segundo.

La evolución de Internet nos ha llevado a la web 2.0 o web social, en la que los usuarios adquieren un papel activo que les permite interactuar con los propios contenidos y espacios virtuales y entre ellos mismos. Este hecho ha marcado un importante punto de inflexión en cuanto a las inferencias del entorno digital con respecto al no virtual. Las plataformas 2.0 se configuran como formas de interacción social basadas en un intercambio dinámico entre los nodos en contextos de complejidad. La red, definida como un sistema abierto y en construcción permanente, involucra a conjuntos que se identifican en las mis-

mas necesidades y problemáticas y que se organizan para potenciar sus recursos (Dron, 2007). En este sentido, apunta el profesor Orihuela (2005) que las redes sociales operan de forma cruzada en tres ámbitos denominados *las 3C*: comunicación (nos ayudan a poner en común conocimientos), comunidad (nos ayudan a encontrar e integrar comunidades) y cooperación (nos ayudan a hacer cosas juntos).

Con todo lo dicho, no extraña que la red se haya convertido en una herramienta y un espacio fundamentales para el propio devenir social y político. Para el ciudadano de la era 2.0, Internet le servirá, por un lado, como una excelente y amplia fuente de información necesaria para conocer su entorno y gestar su propia opinión y, por otro, como espacio interactivo, colaborativo y participativo en el que poner en común las ideas para que estas se nutran mutuamente. A través de una estructura de red distribuida, la web social propicia la participación libre y no jerarquizada de sus usuarios. La web 2.0 ha creado un espacio de comunicación y participación ciudadana en el que se pueden fomentar la cooperación y la ayuda mutua. Este aspecto de los medios sociales (*social media*) hace que sea posible vincular la instauración de Internet con el fortalecimiento de la sociedad civil y la conciencia democrática.

Los ciudadanos están tomando conciencia de que pueden participar en Internet. No obstante, para hacer real la afirmación anterior es precisa la culminación de una alfabetización tecnológica y digital que otorgue las competencias necesarias a la ciudadanía para que esta sea capaz de superar una fase negativa y pasiva y pasar a otra positiva y activa. La alfabetización digital requiere mucho más que saber utilizar las distintas aplicaciones informáticas. Estas destrezas, aunque necesarias, no son suficientes. Hay que ir más allá de la simple alfabetización informática. Se trata de asimilar el uso de las tecnologías de la información y la comunicación (TIC) como base fundamental para el desarrollo y la práctica de las competencias ciudadanas. Por eso, entendemos la alfabetización digital desde un sentido amplio y complejo. Alguien alfabetizado digitalmente debe poseer una serie de características que le permitan ejercer de forma eficaz su papel de ciudadano activo en la sociedad civil.

Metodología

Partimos de la necesidad de indagar las vinculaciones existentes o no entre los movimientos hacktivistas y la libertad de expresión. Es objetivo de este artículo analizar el desarrollo y la situación actual de estas acciones hacktivistas que utilizan técnicas como los ataques tecnológicos o los virus informáticos en pro de determinadas protestas sociopolíticas y de las libertades humanas. A partir de estas interpelaciones nos formulamos los siguientes interrogantes: ¿es

legítimo el uso de técnicas y estrategias ilegales o alegales en pro de la libertad y la defensa de los derechos de las personas?, ¿es necesaria la existencia de estos grupos de presión tecnológica para salvaguardar la libertad de la red?, ¿la respuesta social ante este fenómeno es positiva o negativa?, ¿y la de los gobiernos y organizaciones afectados?, ¿cuál será previsiblemente la evolución de estos movimientos, sus estructuras y actividades?, etc.

En nuestra historia reciente tenemos ejemplos como Anonymous, LulzSec, Gn0sis o RevoluSec, entre otros, que ponen de manifiesto la implantación del ciberespacio como nuevo campo de batalla donde lidiar las luchas cívicas y sociales. Es preciso analizar los objetivos de estos movimientos hacktivistas, examinando la propia naturaleza y vocación de tales colectivos y reflexionando sobre los resultados de sus actuaciones y repercusiones sociales.

Dada la naturaleza compleja de nuestra temática, hemos optado por la utilización de una combinación metodológica cualitativa y cuantitativa a través del desarrollo de un método empírico analítico considerando pautas sistemáticas, sintéticas, deductivas e inductivas. No olvidemos que abordamos el estudio de un fenómeno coetáneo, extraordinariamente cambiante y de difícil delimitación, por lo que nos hemos decantado por una postura abierta conscientes de que nuestro objeto de estudio está en continua relación con la dinámica de cambio en tiempo y espacio.

Entre la libertad y el control: la libertad de expresión y las oportunidades cívicas frente a la censura en red y el control gubernamental

A lo largo de la historia de la humanidad, el ser humano ha evolucionado gracias al surgimiento de nuevos conocimientos. No cabe duda de que el ser humano tiene la capacidad de pensar ni de que esta capacidad es el motor de la evolución y el progreso social. Así fue como pasamos de la Edad de Piedra a la del Bronce, de esta a la del Hierro y así hasta llegar a nuestros días.

En la actualidad se ha puesto en valor ese activo intangible que es el conocimiento y ha llegado a convertirse en uno de los determinantes sociales. De ahí que sea fácil escuchar la catalogación de nuestro momento histórico como el de la sociedad de la información y el conocimiento (SIC). Es más, se suele entender que las TIC son precisamente el antecedente directo de la SIC y que la expresión fundamental de las TIC es Internet, gracias al cual el conocimiento es hoy universalmente accesible y el saber es colectivo y emana de múltiples sitios.

Uno de los principales instrumentos para generar y adquirir conocimiento es, lógicamente, la información. Gracias a las TIC, la transmisión de conocimiento y saberes ha alcanzado unas cotas extraordinarias. Se ha producido una demo-

cratización del saber. Por lo tanto, si aceptamos la premisa de que la información es poder, Internet lo que hace es distribuir ese poder. Pero no debemos confundir información con conocimiento, puesto que, aunque el primero posibilita el segundo, no son lo mismo. La información es, al fin y al cabo, una mercancía que se puede comprar y vender y que tiene más valor cuanto más fresca o actual sea. El conocimiento, por su parte, pertenece a cualquier mente razonable. No es una mercancía que se devalúa o se desgasta. Es un recurso humano y, como tal, su valor aumenta cuanto más se usa. El conocimiento compartido se multiplica en vez de dividirse. Cuando repartimos otros recursos, físicos o financieros, estos se dividen; el conocimiento humano, sin embargo, no se divide, sino que se multiplica.

El valor de Internet radica en su abundancia. Al contrario que otros bienes, como los diamantes, cuya valía está estrechamente relacionada con su escasez, la lógica de la web 2.0 nos dice que la red será más valiosa cuanta más gente tenga acceso a esta e interactúe con el entorno virtual. De ahí que en Internet encontremos gran cantidad de plataformas que propician la creación de conocimiento y capital simbólico. Las redes sociales en la web son estupendos escenarios para el intercambio de información, la colaboración y la resolución de conflictos.

Internet se presenta como una red global con poder de procesamiento de la información y comunicación multinodal, que no distingue fronteras y establece una comunicación irrestricta entre todos sus nodos (Castells, 2001). Resurge con más fuerza un derecho universal que alcanza, o debería alcanzar, su mayor garantía en el ciberespacio: la libertad de expresión. Bustamante (2001) habla de una cuarta generación de derechos humanos, surgida a partir de la inclusión social de las TIC y en la que «la universalización del acceso a la tecnología, la libertad de expresión en la red y la libre distribución de la información juegan un papel fundamental». Ya en la Declaración Universal de los Derechos Humanos de 1948 aparece reconocido el derecho a la libertad de pensamiento, de conciencia y de religión (art. 18), la libertad de investigar y de recibir información (art. 19), y la libertad de opinión y de difundirla sin limitación de fronteras, por cualquier medio de expresión (art. 19). Sin estas libertades se hace imposible la instauración de una sociedad civil activa y participativa dentro de la dinámica de las democracias.

Ahora bien, como afirma Castells (2001), «si la red es global, el acceso es local, a través de un servidor. Y es en este punto de contacto entre cada ordenador y la red global en donde se produce el control más directo». Es decir, si «técnicamente, Internet es una arquitectura de libertad, socialmente, sus usuarios pueden ser reprimidos y vigilados». En efecto, no son pocas las medidas y estrategias llevadas a cabo por los diferentes gobiernos y grupos de poder para

controlar y vigilar los espacios en línea. Para Cáceres (2004), los distintos gobiernos de diversas ideologías y regímenes políticos se han valido del pretexto de defender la seguridad nacional o de preservar la unidad o valores nacionales para impedir a sus ciudadanos un acceso libre a Internet. Así lo corrobora el informe *Enemigos de Internet*, elaborado por Reporteros Sin Fronteras (2014), que revela que algunos organismos gubernamentales y agencias implementan la censura y la vigilancia en línea. Los casos más extremos los hallamos en organismos como la Autoridad de Telecomunicaciones del Pakistán, el Centro Científico y la Agencia de Información Tecnológica de Corea del Norte, el Ministerio de Información y Comunicaciones de Vietnam o la Oficina Estatal de Información de Internet de China, que han usado la defensa de la seguridad como pivote para ir mucho más allá de su misión original con el fin de censurar a periodistas, blogueros y otros proveedores de información.

Pero tales actuaciones también las encontramos, según este informe, en democracias que tradicionalmente se han jactado de defender la libertad de expresión y el libre flujo de información. Así, podemos citar a la NSA (Agencia de Seguridad Nacional) en Estados Unidos, el GCHQ (Cuartel General de Comunicaciones del Gobierno) en el Reino Unido o el Centro de Desarrollo Telemático de la India. También es polémica la herramienta SITEL (Sistema Integrado de Interceptación de Telecomunicaciones) puesta en marcha en 2001 en España y que permite al Gobierno interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis. El programa lo controla el Ministerio del Interior, lo utilizan indistintamente la Guardia Civil, el Cuerpo Nacional de Policía y el Centro Nacional de Inteligencia y su aplicación requiere de la imprescindible colaboración de las operadoras privadas (Lobo, 2013).

En todo este entramado se precisa de la ayuda de las empresas del sector privado que funcionan como facilitadoras de información y datos a los organismos solicitantes incluso antes de haber una orden judicial. Reporteros Sin Fronteras (2014) critica duramente a «las compañías que ponen sus conocimientos al servicio de los regímenes autoritarios a cambio de sumas de dinero a menudo colosales». Del mismo modo, Pete Ashdown, fundador de XMission, denunció que «gigantes como Google, Microsoft o Apple seguramente se benefician económicamente al permitir que la NSA obtenga datos de sus redes» (Ashdown citado en *Russia Today*, 2013).

Las redes sociales también se han convertido en puntos de interés estratégicos para los gobiernos y agencias que no dudan en establecer solicitudes de información sobre sus internautas. En este sentido, y en un intento de ofrecer transparencia y confianza a sus usuarios, el gigante Facebook publica periódi-

camente informes sobre las solicitudes de los gobiernos en los que se detallan los siguientes datos: países que solicitaron a Facebook información sobre los usuarios; número de solicitudes recibidas de cada uno de esos países; número de usuarios/cuentas de usuario especificados en esas solicitudes, y porcentaje de solicitudes en las que Facebook estaba obligado por ley a revelar al menos algunos datos (Facebook, 2013). Hasta la fecha ha publicado dos informes, correspondientes al primer y segundo semestres de 2013, y en ambos Estados Unidos es el país que más peticiones ha tramitado: en torno a 24.000 a lo largo del pasado año y de las cuales fueron atendidas el 80 %, aproximadamente (Facebook, 2014).

Del ciberactivismo al hacktivismo: diferencias entre ambos movimientos en red

Cada momento histórico y contexto social ha precisado de técnicas y estrategias de participación propias. El activismo ha sido una constante a lo largo de la historia que sigue presente hoy día pero que se ha transformado o integrado con las nuevas fórmulas de comunicación y participación sociales. Los nuevos medios reformulan el concepto de ciudadanía y exigen nuevas formas de participación democrática. El contexto en red crea nuevos entornos intelectuales y simbólicos, el ciberespacio fomenta imaginarios colectivos, identidades y conflictos sociales. De forma paralela, articula nuevas vías de acción y de actuación ciudadana, como una ampliación de la ciudadanía y sociedad civil.

De este modo, el activismo tradicional se integra en la esfera digital y utiliza las herramientas tecnológicas para la consecución de sus objetivos. Observamos un cambio drástico en la secuencia de los pasos a llevar a cabo por los activistas: si en el mundo del viejo activismo la organización es previa a la difusión, con el advenimiento de Internet y la web 2.0 se configura un ciberactivismo en el que no es necesario construir ninguna red para transmitir, pues ya viene configurada por el propio contexto en línea (Ugarte, 2006). Es decir, la organicidad de los procesos sociales colectivos se difunde en una estructura desjerarquizada y autoorganizada. Los movimientos surgidos en la red se basan en estructuras horizontales en las que no hay cúpula ni poder jerárquico y todos los miembros tienen un papel igualitario. De acuerdo con Ugarte (2008), en la cibermovilización no hay una dirección consciente ni centralizada y es imposible encontrar un organizador o un grupo dinamizador responsable y estable; como mucho, podemos hablar de *propositores* originales que se irán disolviendo poco a poco en el propio movimiento.

Estas nuevas movilizaciones toman como punto de partida la esfera en línea, en la que los individuos encuentran un espacio para compartir preocupaciones

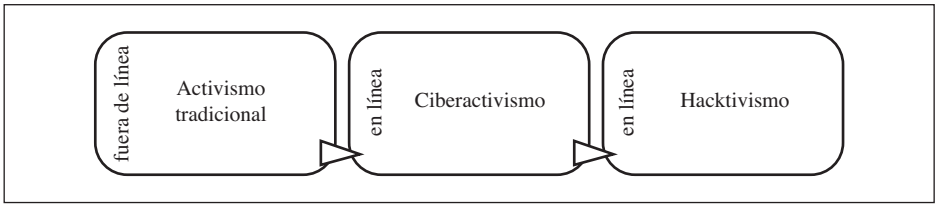

FIGURA 1. Evolución del activismo fuera de línea al activismo en línea.
FUENTE: Elaboración propia.

y facilitan así el encuentro de esas personas con inquietudes comunes que han hecho de la red una eficaz herramienta de discusión y movilización. Internet se ha convertido en un arma de crucial importancia en estos procesos movilizadores por su poder de difusión, de convocatoria y de movilización. Adolfo Plasencia (2011) se refería así a la importancia de las TIC y los entornos 2.0 en la gestación y el desarrollo de la Primavera Árabe: «en el París de Mayo del 67 los manifestantes más aguerridos llevaban en sus manos adoquines y cócteles molotov para enfrentar el poder de la policía. En Túnez y Egipto llevaban *smartphones* con cámara, teclado y conexión móvil a Internet».

Las manifestaciones ciberactivistas se caracterizan por una gran informalidad y espontaneidad en su formación y estructura, ya que utilizan los medios digitales como un arma de difusión de mensajes que propulsa acciones concretas. En la gestación de estas movilizaciones existen tres etapas correlativas: la deliberación, la convocatoria y la actuación. Dependiendo de la repercusión, la importancia y el número de seguidores, una iniciativa surgida en la red puede quedarse en la primera etapa, avanzar hasta la segunda y, en algunos casos, culminar en la tercera.

La primera de ellas es una fase previa deliberativa, de debate y discusión, en la que los usuarios en red plantean un asunto problemático, lo tratan, lo estudian, conversan acerca de él y de sus posibles soluciones, etc. Consiste, sobre todo, en poner de relieve la cuestión conflictiva, presionando a los agentes políticos, sociales y/o mediáticos para que actúen en este sentido. A veces, el activismo en red puede permanecer mucho tiempo inserto en esta fase e incluso no superarla si no se dan las circunstancias necesarias. No obstante, es muy común que los usuarios enzarzados en una causa utilicen las plataformas interactivas para dar un paso más y realizar cualquier tipo de actuación que le dé mayor notoriedad al problema en cuestión. Para ello es necesario entrar en la segunda etapa, utilizando el medio de Internet para divulgar la convocatoria y aunar adeptos.

Las redes sociales digitales poseen una gran capacidad de convocatoria, consecuencia lógica de su potencial difusor. Actúan como un elemento viral y si-

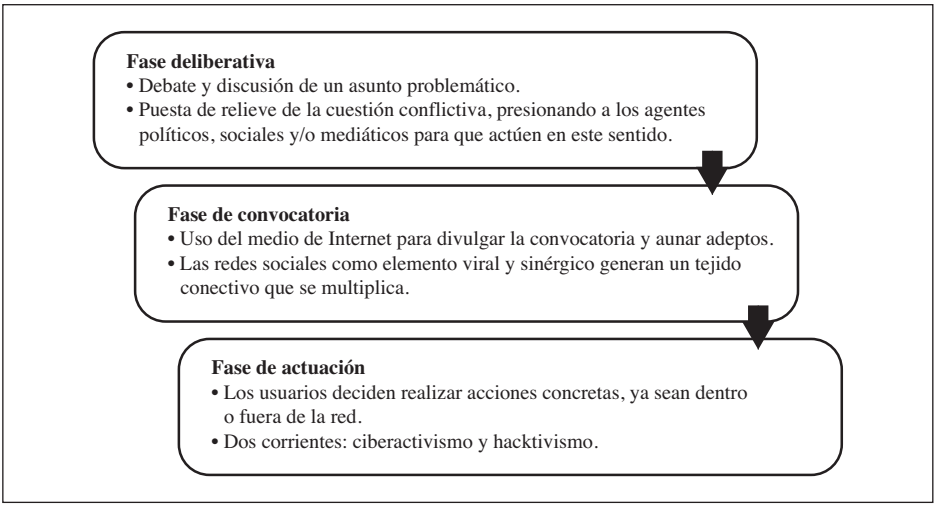

FIGURA 2. Fases en la gestación de las movilizaciones en red.
FUENTE: Elaboración propia.

nérgico generando un tejido conectivo que tiene la propiedad de multiplicarse. La facilidad y rapidez de propagación que presenta la web social consiguen que el mensaje se convierta en «contagioso» y se extienda como si de una epidemia de gripe se tratara (Aced, Arqués, Benítez, Llodrá y Sanagustín, 2009: 85). Este contagio se hace efectivo, puesto que en las redes sociales el mensaje es transmitido de una persona concreta a sus contactos, por lo que estos sienten mayor vinculación hacia la fuente, con un consiguiente aumento de interés. Se forma así una «ideavirus» que se mueve, que crece y que infecta todo lo que toca (Godin, 2001: 19).

Una vez superada con éxito la segunda fase se alcanza la tercera, en la que los usuarios deciden realizar acciones concretas, ya sean dentro o fuera de la red. Aquí radica la principal diferencia entre el ciberactivismo, que toma su expresión normalmente en la calle, y el hacktivismo, que utiliza el mismo entorno cibernético como escenario en el que actuar. Los movimientos gestados desde el prisma del ciberactivismo suelen desembocar en revueltas callejeras, movilizaciones espontáneas y masivas de diferente índole. Es lo que Ugarte (2008: 66) denomina con el concepto de ciberturbas, que pueden adquirir diversas formas (las más comunes son las manifestaciones, las quedadas, las sentadas, las reuniones, etc.). Ejemplos actuales en los que el ciberactivismo ha tenido una importancia crucial han sido todas las revueltas acaecidas en Oriente Medio o las manifestaciones del 15M y el movimiento Democracia Real Ya en España.

El hacktivismo, por su parte, emplea otros métodos para presionar y conseguir sus objetivos. Suelen ser usuarios con conocimientos informáticos avanzados, con un extraordinario manejo de las TIC y de las redes, y con habilidad para inventarlas, redefinirlas y modificarlas. Para los hacktivistas, el ciberespacio no es solamente el nuevo escenario de empoderamiento civil, sino el nuevo campo de batalla global cuya protesta viral se ejerce a través de la acción cibernética.

Movimientos hacktivistas: objetivos y actuaciones

El término *hacktivismo* fue usado por primera vez en un artículo de la artista multimedia Shu Lea Cheang publicado en *InfoNation* en 1995; un año después, sería utilizado por un miembro del grupo de *hackers* americano Cult of the Dead Cow (cDc). Pero será en el año 2000 cuando Oxford Ruffin, otro miembro del citado grupo, escriba que «los hacktivistas emplean tecnología para defender los derechos humanos» (Paget, 2012: 3).

Podemos definir el hacktivismo como «la utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de *software*» (Samuel citado en «Hacktivismo» en *Wikipedia*, 2014). El hacktivismo combina, pues, elementos del *hacking online* y del activismo político (Denning, 2003).

El hacktivismo es un tipo de activismo en red que emplea el *hacking* como principal técnica para luchar por una causa política (Denning, 1999). Aunque a menudo se redactan y se distribuyen comunicados, declaraciones de principios y manifiestos, su fuerza no se limita a la retórica, pues estos discursos van acompañados de acciones concretas que toman su expresión en el entorno digital. Los hacktivistas adoptan estrategias y herramientas más directas y transgresoras que las usadas por el ciberactivismo, puesto que creen que sus tácticas de confrontación son más eficaces que las fórmulas convencionales. Estas acciones tienen un carácter creativo y performativo: creativo en tanto que generan artefactos culturales nuevos y performativo porque dichos artefactos realizan los valores y principios que guían la acción (Aceros, 2006).

Este movimiento contracultural del siglo XXI tiene su origen en la década de los años setenta del pasado siglo, cuando los *hackers* de entonces deciden romper con la dinámica imperante de ocultación y privatización del *software* y luchar por la liberalización de este, como un paso previo e imprescindible para combatir el cibercontrol social (Garaizar, 2005) y batallar por la libertad del conocimiento y la justicia social. Se suelen relacionar con la idea de la desobediencia civil electrónica (DCE) dentro de la resistencia digital. La DCE es una

propuesta del grupo Critical Art Ensemble (1995) que, bajo la consigna de «ofender y bloquear», plantea el bloqueo de los flujos de información que resultan útiles a los centros de poder.

Confían en el valor social y político de la tecnología fomentando un hackerismo que va mucho más allá del placer de experimentar con las TIC y aprender de ello. Entienden que la tecnología se ha convertido en un mediador necesario para la emergencia de nuevas formas de sociabilidad (Aceros, 2006). El mundo del *software* tiene implicaciones sociales, con el compromiso ciudadano de acercar «herramientas de interacción tecnopolíticas a la gente corriente» (Garaizar, 2005: 10). Así, el uso político que hacen los hacktivistas les diferencia del *hacker*, ya que, normalmente, este último es «un personaje apolítico que solo lucha por sus compañeros, por la libertad de la información y por sí mismo» (Vicente, 2004). En cambio, para los hacktivistas los puntos de partida coinciden con los principios consagrados en la Declaración Universal de los Derechos Humanos y la Convención Internacional sobre Derechos Civiles y Políticos. Tampoco podemos vincular estos movimientos hacktivistas con los *crackers*, «cuyo objetivo es el de crear virus e introducirse en otros sistemas para robar información y luego venderla al mejor postor» (Vicente, 2004). De igual forma, surge en el seno del hacktivismo una escisión que se aleja del compromiso cívico y de la que resultan los conocidos *script kiddies*, jóvenes que intentan hacerse pasar por *hackers*, a pesar de su falta de habilidades técnicas y experiencia en sistemas informáticos, y con ganas de «piratear por piratear» (Paget, 2012: 9).

Las incipientes actuaciones hacktivistas estuvieron protagonizadas por grupos como Electronic Disturbance Theatre, Electrohippies, Cult of the Dead Cow, Hactivist.com, Critical Art Ensemble o HispanoTecno.Net. Desde mediados de los años noventa se han llevado a cabo una serie de acciones concretas hacktivistas con un predominio de *hacklabs* y *hackmeetings*, instancias de diálogo de *hackers* que lo consolidan como un movimiento social articulado dentro y fuera de la red. Desde el punto de vista de las estructuras sociales, estos movimientos canalizan su acción en tres dimensiones: la solidaridad, es decir, el mutuo reconocimiento de los actores como miembros de una misma unidad social; el conflicto con un adversario por la apropiación y el control de recursos valorados por ambos, y la ruptura de los límites de compatibilidad del sistema en el que acontece la movilización (Melucci, 1999).

Las primeras acciones hacktivistas fueron conocidas como *netstrikes*, que consistían en organizar manifestaciones de protesta en red a través del bloqueo de determinadas páginas web. Mediante un programa muy sencillo, utilizable desde cualquier ordenador personal, un hacktivista realiza continuas peticiones a una misma página web intentando colapsarla. Este ataque combinado desde

TABLA 1. Tipos de hacktivismo, resumido por características

	Formas	*Orígenes*	*Orientación*	*Temática*	*Cuándo*
Cracking político	Desfiguración Redirección Ataques de denegación de servicios Sabotaje Información Robo	Programadores *hackers*	Fuera de la ley	Cuestiones en línea que abarcan gradualmente cuestiones fuera de línea	Desde la década de los noventa
Hacktivismo performativo	Parodias Sentadas	Artistas activistas	Transgresor	Cuestiones fuera de línea	Desde 1997
Codificación política	Desarrollo de *software*	Programadores *hackers*	Transgresor	Cuestiones fuera de línea	Desde 1999

FUENTE: Samuel (2004: 101).

diferentes fuentes puede perjudicar seriamente la accesibilidad de un sitio web. Uno de los casos más sonados fue el coordinado por la web italiana *Netstrike.it*, cuando en 1995 consiguió bloquear los sitios del Gobierno francés que en aquel momento estaban realizando ensayos nucleares en el atolón de Mururoa.

El movimiento Anonymous

En la actualidad, al hablar de hacktivismo debemos hacer mención especial al movimiento Anonymous por la repercusión de sus actuaciones, su ámbito de acción y su prolongación en el tiempo. Anonymous es un grupo *hacker* que muestra como símbolo una máscara con el rostro del anarquista revolucionario Guy Fawkes, emblema que se ha popularizado recientemente con la película de 2006 *V de Vendetta*, protagonizada por Natalie Portman y Hugo Weaving y basada en la novela gráfica de Alan Moore. Su lema, «Somos una legión, no perdonamos, no olvidamos, espéranos. Anonymous», refleja el espíritu revolucionario y activista de este movimiento sin líderes ni portavoces.

Anonymous se configura como una subcultura nacida de Internet que agrupa a personas que no pertenecen a ninguna asociación pero que se unen para realizar determinadas protestas y acciones. Un fenómeno sociocultural y político compuesto por ciudadanos de todo el mundo, que no se conocen entre ellos y en el que todos participan coordinadamente y de forma anónima.

Operan como una conciencia compartida basada en Internet, una voluntad colectiva que resulta de la combinación de voluntades individuales. Su lucha está encaminada en contra de los excesos del poder, de las operaciones encu-

biertas de los gobiernos, del oscurantismo político y económico, de los actos ilegales, de las actividades fraudulentas y de las violaciones a los derechos humanos. Pretenden un aumento de las libertades, los derechos civiles, la participación activa y la defensa del conocimiento compartido, la innovación abierta y la libertad de expresión y de pensamiento.

Aunque sus orígenes son más lejanos, el punto de inflexión que le otorgó relevancia social fue el conocido como Proyecto Chanology, en 2008, en relación con la Iglesia de la Cienciología, y un vídeo que había sido censurado de YouTube en el que aparecía Tom Cruise exhibiendo las virtudes de este culto. A partir de aquí, existe un largo listado de proyectos y operaciones contra la censura en Internet, las injusticias sociales y en pro de la libertad del individuo y sus derechos fundamentales.

Anonymous se organiza en toda la red. No hay sitios oficiales ni foros representativos de este movimiento. Se trata de una cultura cibernética cuyo entorno es Internet en su totalidad, una red descentralizada y distribuida en la que no cabe un orden establecido ni jerarquía. Es por ello que muchos asemejan la estructuración del movimiento Anonymous con una especie de ciberanarquismo activista, en el sentido de que existe una igualdad total entre sus miembros, sin la primacía de líderes ni reguladores. Sin embargo, la experiencia ha mostrado que el aspecto anárquico de Anonymous no significa que carezca de una serie de normas, valores, creencias y acciones, así como una coordinación espontánea pero efectiva que le permite llevar a cabo sus acciones.

Principales operaciones y otros movimientos

El hacktivismo está a favor de la libertad de expresión y el derecho a la información y en contra de cualquier tipo de control y censura en la red. Por eso, cuando WikiLeaks empezó a publicar cables diplomáticos estadounidenses comprometedores y, a su vez, los poderes políticos iniciaron los intentos de callar la *wiki* de Julian Assange, los movimientos como Anonymous decidieron intervenir y convertirse en el intermediario entre el público y los denunciantes (Paget, 2012: 7). Se inauguraba así, el 28 de noviembre de 2010, la operación Cablegate. Surgieron toda clase de operaciones con el fin de defender WikiLeaks y difundir sus cables. El grupo de *hackers* RevoluSec también llevó a cabo operaciones para deformar sitios webs oficiales. Posteriormente, el 6 de diciembre de ese año, cuando compañías como PostFinance o PayPal bloquearon las cuentas de WikiLeaks, Anonymous volvió a salir en su defensa a través de una operación Payback.

Otro acontecimiento destacado lo protagonizó Aaron Barr, CEO de HBGary Federal, que declaró al periódico *The Financial Times* que tenía la intención de

proporcionar al FBI la información que había reunido sobre Anonymous y que quería eliminar a sus principales protagonistas. El grupo comenzó a atacar de inmediato los servidores de su empresa. La asimetría de esta ciberguerra se hizo evidente y Barr vio cómo su compañía de seguridad bien financiada, con una historia y con fuertes capacidades cibernéticas ofensivas, fue derrotada por un colectivo de *hackers* sin finanzas y poco organizado (Meer, 2011).

En el año 2011 viviríamos la reconciliación entre un colectivo de hacktivistas derivados del grupo Gn0sis y reagrupados bajo el nombre de Lulz Security (LulzSec) y Anonymous. Los integrantes de Gn0sis prefieren la diversión de mal gusto (conocido como *lulz*) al activismo, por lo que existía una disputa entre ambos grupos. Sin embargo, el 17 de julio de 2011 LulzSec celebró su tuit número 1.000 y anunció el fin de su rivalidad con Anonymous. Dos días después, ambos movimientos iniciaron conjuntamente la operación AntiSec contra las directivas de seguridad de los gobiernos que pretenden limitar la libertad de expresión en la red (Paget, 2012: 13).

Una vertiente de Anonymous más ecologista y comprometida con el medio ambiente organizó la operación Green Rights, especialmente tras el tsunami y el desastre nuclear de Fukushima, ocurrido el 11 de marzo de 2011.

Estos movimientos y su simbología han sido también interpretados y manifestados en recientes expresiones ciudadanas y revolucionarias como el movimiento de los indignados en España en mayo de 2011 o el Occupy Movement estadounidense. Poco antes, en enero de ese año, con el estallido de la Primavera Árabe el grupo Telecomix, creado en abril de 2009 en Suecia y gestado bajo el principio llamado *do-ocracy* (estructura flexible en la que los individuos autoseleccionan las tareas a llevar a cabo), restableció parcialmente el acceso a la web en Egipto y repitió la misma operación en Libia en febrero de 2011.

Técnicas de actuación y vías de comunicación hacktivista

Las técnicas empleadas por los grupos hacktivistas son diversas y variadas, en función de los objetivos, de los agentes implicados, de la naturaleza de la reivindicación, etc. En general, podemos establecer una tipología básica que suelen regir las características y dinámicas de acción de estos colectivos:

— Un ataque DDoS (*distributed denial of service attack* o ataque distribuido de denegación de servicio) es una técnica *hacker*, bastante antigua en el mundo del ciberespacio, consistente en un ataque a un sistema de computadoras o red que provoca que un servicio o recurso sea inaccesible para los usuarios legítimos. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina *denegación*, pues hace que el servidor no dé abasto a la

cantidad de solicitudes. La forma más habitual de este tipo de ataques se realiza a través de programas informáticos bastantes sencillos (como LOIC) que permiten entrar gran cantidad de veces a un sitio web en concreto de forma automatizada y con una identidad falsa (*botnets*), de forma que, al realizar tal volumen de peticiones de datos a un servidor y desde tantos puntos al mismo tiempo, estos intentos de conexión consumen recursos en el servidor, limitan el número de conexiones que se pueden hacer y reducen la disponibilidad del servidor para responder a otras peticiones legítimas de conexión.

— Los ataques *netstrike* consisten en la interacción consensuada de multitud de personas desde diferentes lugares y distintos horarios sobre un sitio web, con el objetivo de ralentizar su servicio, llegando en ocasiones a saturar la web. En este caso los atacantes son personas conscientes de su acción, al contrario que en el caso del ataque anterior, para el que se emplean en su mayoría *zombies* (ordenadores que atacan automáticamente a través de algún virus o troyano).

— Se utilizan *exploits*, fragmentos de *software* o secuencias de comandos y/o acciones, con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado de este.

— El *doxing* consiste en publicar fotos, información de contactos y datos personales y familiares en represalia por una acción llevada a cabo por un individuo o grupo de individuos.

— El *copwatching* permite publicar en sitios web especiales información identificativa y observaciones relacionadas con los miembros de las fuerzas de seguridad.

— El *Google bomb* es un método mediante el cual es posible colocar ciertos sitios web en los primeros lugares de los resultados de una búsqueda en Google utilizando un texto determinado.

— Los *fakes* son falsificaciones o engaños que pretenden suplantar una institución o campaña oficial el mayor tiempo posible.

— Redirección de las páginas web institucionales u oficiales.

— Desarrollo de herramientas de *software* (*rootkits*, *keyloggers*, etc.).

— Robo de datos y filtraciones, a través de ataques de inyección SQL, por ejemplo.

En cuanto a las vías establecidas para la comunicación entre los propios miembros de los movimientos hacktivistas preocupa especialmente la seguridad y la ocultación de la identidad, por lo que es importante no dejar rastro de la IP. Para ello suelen emplear métodos como la red privada virtual (RPV); la I2P, que es una red que permite «anomizar», o los *proxies* como TOR (The Onion Router), que son conexiones intermediarias que permiten ocultar la IP y acceder a sitios webs restringidos. Es muy común que estos usuarios también empleen de forma periódica y frecuente cuentas de correo temporales/desechables de

proveedores como Guerrillamail.com, Trashmail.com, 10minutemail.com o Sofortmail.de.

Ahora bien, la principal manera de contactar empleada por los hacktivistas es a través de los canales IRC, sistemas de chat multicanal cuyos canales conversacionales suelen ir designados por nombres que habitualmente comienzan con el carácter # (*#hispano* para la versión española de Anonymous, por ejemplo). Además, IRC autoriza la adquisición del *software* LOIC para los ataques DDoS.

De igual forma, estos colectivos, especialmente Anonymous, suelen realizar vídeos que difunden en plataformas como YouTube para explicar sus actuaciones, asignarse autorías o denunciar situaciones. Además, también son usuarios y emplean redes sociales como Facebook o Twitter, entre otras.

Conclusiones

Internet y sus plataformas se han configurado como importantes espacios de encuentro y debate en los que los usuarios pueden compartir información, comentarios, opiniones e inquietudes. La web social se nutre de esta inteligencia colectiva gestada en comunidad y liberada en un espacio digital libre y abierto. Ahora bien, es evidente que no son pocos los intentos de los gobiernos y agencias oficiales por controlar, e incluso censurar, los contenidos allí alojados y la propia actividad de los usuarios.

Todo ello sitúa al ciberespacio como un elemento crucial en el desarrollo del nuevo tejido social y sus implicaciones cívicas y políticas. No cabe duda de que en la actualidad el entorno web se ha convertido en una importante herramienta para ejercer y desarrollar el activismo social. En este contexto han surgido grupos que entienden que el alcance de la tecnología va más allá de un mero medio y están convencidos del valor cívico y político del *software* en la construcción social. Apuestan por la privacidad y el acceso libre a la información y desconfían de las normas y exigencias que provienen de autoridades externas y que pretender regular la red.

Nacen así movimientos hacktivistas como Anonymous, que no debemos confundir con los *hackers* ni los *crackers* informáticos, ya que, si bien todos tienen altas habilidades y competencias sobre los sistemas de redes, solo los primeros adoptan un verdadero compromiso social de denuncia y de cambio. Abogan por la libertad de expresión y del conocimiento, el derecho a la información, los derechos de los individuos y la justicia social. Los hacktivistas están convencidos de que desde el ciberespacio se pueden desarrollar los grandes cambios sociales y confían en sus técnicas y estrategias para ello. No obstante, el carácter no poco conflictivo de sus actuaciones pone en tela de juicio sus actos y han propiciado una fuerte escisión en la opinión pública y los agentes cívicos y

sociales (entre unos defensores acérrimos que defienden la calidad y voluntad de estas actuaciones y unos detractores que se oponen a ellas).

Bibliografía

ACED, Cristina; ARQUÉS, Neus; BENÍTEZ, Magalí; LLODRÁ, Bel; SANAGUSTÍN, Eva. *Visibilidad: Cómo gestionar la reputación en Internet*. Barcelona: Gestión 2000, 2009.

ACEROS, Juan Carlos. *Jóvenes, hacktivismo y sociedad de la información* [en línea]. Barcelona: Universitat Autònoma de Barcelona, 2006. <http://www.sindominio.net/metabolik/alephandria/txt/Aceros_-_Juventud_hacktivismo_y_sociedad_de_la_informacion.pdf> [Consulta: 19 agosto 2011].

BUSTAMANTE, Javier. «Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica». *Revista Iberoamericana de Ciencia, Tecnología e Innovación* [en línea], 1 (2001). <http://www.oei.es/revistactsi/numero1/bustamante.htm> [Consulta: 18 mayo 2011].

CÁCERES, Sebastián. «Censura y control de contenidos de internet en el mundo». *Observatorio de la Sociedad de la Información, Fundación Orange* [en línea] (2004). <https://es.calameo.com/read/0045516289e42bbf3ee87> [Consulta: 11 marzo 2014].

CASTELLS, Manuel. «Internet: ¿una arquitectura de libertad? Libre comunicación y control del poder». *Internet y comunicación* [en línea]. Barcelona: Universitat Oberta de Catalunya, 2001. <http://www.uoc.edu/web/esp/launiversidad/inaugural01/internet_arq.html> [Consulta: 14 febrero 2014].

CRITICAL ART ENSEMBLE. *Electronic civil desobecience* [en línea]. 1995. <http://www.critical-art.net/books/ecd/index.html> [Consulta: 11 marzo 2009].

DENNING, Dorothy E. *Activism, hacktivism, and cyberterrorism*: *The internet as a tool for influencing foreign policy*. Berkeley, California: Nautilus Institute, 1999.

— «Activismo, hacktivismo y ciberterrorismo: Internet como instrumento de influencia en política exterior». En: ARQUILLA, John; RONFELDT, David. *Redes y guerras en red*: *El futuro del terrorismo, el crimen organizado y el activismo politico*. Madrid: Alianza Editorial, 2003.

DRON, Jon. «Designing the undesignable: social software and control». *Educational Technology & Society*, 10, 3 (2007), p. 60-71.

ECHEVERRÍA, Javier. *Los señores del aire: Telépolis y el tercer entorno*. Barcelona: Destino, 1999.

FACEBOOK. «Informe de solicitudes de gobiernos» [en línea]. 2013. <https://www.facebook.com/about/government_requests> [Consulta: 1 abril 2014].

— «Informe sobre solicitudes gubernamentales» [en línea]. 2014. <https://govtrequests.facebook.com/> [Consulta: 1 abril 2014].

GARAIZAR, Pablo. «El *software* libre como herramienta de hacktivismo contra el cibercontrol social». En: *Solidaridad en red*: *Nuevas tecnologías, ciudadanía y cambio social*. Bilbao:

Hegoa, 2005. También disponible en línea en <http://paginaspersonales.deusto.es/garaizar/papers/HEGOA2004-PG.pdf> [Consulta: 14 agosto 2011].

GODIN, Seth. *Unleashing the ideavirus*. Nueva York: Hyperion, 2001.

«Hacktivismo». En: *Wikipedia* [en línea] (2014). <http://es.wikipedia.org/wiki/Hacktivismo> [Consulta: 12 marzo 2014].

LOBO, José Luis. «¿Nos espía Rajoy? El Gobierno escruta sin control judicial llamadas y correos electrónicos». *El Confidencial* [en línea] (5 julio 2013). <https://www.elconfidencial.com/espana/2013-07-05/nos-espia-rajoy-el-gobierno-escruta-sin-control-judicial-llamadas-y-correos-electronicos_195459/> [Consulta: 6 julio 2013].

MEER, Haroon. «Lecciones de Anonymous sobre la guerra cibernética». *Rebelión* [en línea] (2011). <http://www.rebelion.org/noticia.php?id=124068> [Consulta: 23 septiembre 2013].

MELUCCI, Alberto. *Acción colectiva, vida cotidiana y democracia*. México: El Colegio de México: Centro de Estudios Sociológicos, 1999.

ORIHUELA, José Luis. «Apuntes sobre redes sociales». *eCuaderno* [en línea] (19 julio 2005). <http://www.ecuaderno.com/2005/07/19/apuntes-sobre-redes-sociales> [Consulta: 20 enero 2011].

PAGET, François. «Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas». *Scribd* [en línea]. 2012. <https://www.scribd.com/document/99261543/El-ciberespacio-Nuevo-medio-de-difusion-de-ideas-politicas> [Consulta: 12 febrero 2014].

PLASENCIA, Adolfo. «Sobre Internet y las redes sociales, escenario y arma de las nuevas revoluciones». *El Blog de Adolfo Plasencia* [en línea] (6 marzo 2011). <http://adolfoplasencia.es/blog/sobre-internet-y-las-redes-sociales-escenario-y-arma-de-las-nuevas-revoluciones/> [Consulta: 6 marzo 2011].

REPORTEROS SIN FRONTERAS. «Enemigos de Internet». *RSF* [en línea] (2014). <http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/> [Consulta: 24 abril 2014].

RUSSIA TODAY. «Google, Microsoft y Apple se benefician de entregar datos al Gobierno de EE. UU.». *RT* [en línea] (11 julio 2013). <http://actualidad.rt.com/actualidad/view/99703-google-microsoft-apple-eeuu-espionaje> [Consulta: 15 julio 2013].

SAMUEL, Alexandra. *Hacktivism and the future of political participation* [en línea]. Tesis doctoral. Cambridge, Massachusetts: Harvard University, 2004. <http://www.alexandrasamuel.com/dissertation/pdfs/index.html> [Consulta: 11 octubre 2013].

UGARTE, David de. «Del activismo al ciberactivismo: un viaje de ficción». *El Correo de las Indias* [en línea] (23 enero 2006). <https://lasindias.com/del-activismo-al-ciberactivismo-un-viaje-de-ficcion> [Consulta: 11 noviembre 2012].

— *El poder de las redes* [en línea]. 2008. <http://www.pensamientocritico.org/davuga0313.pdf> [Consulta: 14 abril 2010].

VICENTE, Loreto. «¿Movimientos sociales en la Red? Los hacktivistas». *El Cotidiano* [en línea], 20, 126 (2004). <http://www.redalyc.org/pdf/325/32512615.pdf> [Consulta: 16 noviembre 2013].

Datos de la autora

Noelia García Estévez es profesora de la Facultad de Comunicación de la Universidad de Sevilla. En 2013 defendió su tesis doctoral *Presencia de las redes sociales y medios de comunicación: representación y participación periodística en el nuevo contexto social*.