LA NEBULOSA DEL ICEBERG CIBERNÉTICO: ENTRE LA LIBERTAD Y EL OCULTISMO

NEBULA CYBER ICEBERG: BETWEEN FREEDOM AND THE OCCULT

Noelia García Estévez
Universidad de Sevilla
noeliagarcia@us.es

Resumen: Este artículo contribuye a la comprensión del actual tejido social y las dinámicas de activismo tecnológico llevadas a cabo desde y en Internet. Las nuevas formas de acción colectiva se basan en una Internet abierta, libre y descentralizada. Ahora bien, algunos derechos fundamentales tales como la privacidad y la intimidad o la libertad de expresión y la libre circulación de ideas se están encontrando ciertas trabas en el medio digital. La *deep web* se presenta como el entorno idóneo donde ciudadanos nacidos de la era *hacker* y bajo el influjo de la cultura libre se organizan en grupos *hacktivistas* y ejercen presión a los poderes económicos y políticos. La metodología empleada incluye la revisión bibliográfica así como un trabajo de campo y una observación participante en los entornos estudiados. Los resultados confirman que se está imponiendo el valor cívico y político del software como elemento clave en la construcción social. Grupos de activismo tecnológico como Anonymous están adquiriendo mayor importancia y protagonismo en el devenir social, político y económico.

Palabras clave: *Hacktivismo*, activismo, *deep web*, Internet, software libre, Anonymous, tecnología.

Abstract: *This article contributes to the understanding of modern society and the dynamics of technological activism undertaken from and on the internet. The new forms of collective action are based on an open, free and decentralized internet. However, fundamental rights such as privacy and intimacy or freedom of expression and the free flow of ideas are encountering some obstacles in the digital medium. The deep web is presented as the ideal environment where citizens born of the hacker era and under the influence of free culture are organized in hacktivist groups and exert pressure on the economic and political powers. The methodology for this study includes a bibliographical review, fieldwork and participant observation in the environments studied. The results confirm that technological activism is imposing civic and political value of software as a key element in social construction. Technological activist groups such as Anonymous are gaining importance and prominence in the social, political and economic future.*

Key words: *Hacktivism, activism, deep web, internet, free software, Anonymous, technology.*

Recibido: 06/10/2014 Aceptado: 20/01/2015 • Anduli • Nº 13 - 2014 • 43-58 • ISSN 16960270
• Nº DOI: http://dx.doi.org/10.12795/anduli.2014.i13.03 •

1. Introducción

Vivimos en una era tecnológica donde 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 daban en los entornos primero y segundo.

La evolución de Internet nos ha llevado a la web 2.0 o web social, donde los usuarios adquieren un papel activo que les permite interactuar con los propios contendidos 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 mismas 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 3Cs": de comunicación (nos ayudan a poner en común conocimientos), de comunidad (nos ayudan a encontrar e integrar comunidades) y de cooperación (nos ayudan a hacer cosas juntos).

Con todo lo dicho, no extraña que la red se haya convertido en una herramienta y 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 donde poner en común las ideas para que éstas 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 puede fomentar la cooperación y ayuda mutua. Este aspecto de los social media hacen que sea posible vincular la instauración de Internet con el fortalecimiento de la sociedad civil y la conciencia democrática.

Los ciudadanos en Internet están tomando conciencia de que pueden participar. No obstante, para hacer real la anterior afirmación es preciso la culminación de una alfabetización tecnológica y digital que le otorgue las competencias necesarias a la ciudadanía para que ésta se capaz de superar una fase negativa y pasiva hacia 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 TIC como base fundamental para el desarrollo y práctica de las competencias ciudadanas. Por eso, entendemos la alfabetización digital desde un

sentido amplio y complejo. Una persona alfabetizada digitalmente debe poseer una serie de características que le permitan ejercer de forma eficaz su papel de ciudadano activo en la sociedad civil.

Hoy día nada es igual que antes de la llegada de Internet. Para Candón Mena existen seis movimientos nacidos como consecuencia de esta irrupción tecnológica con implicaciones comunicativas y sociales: la defensa de la red como bien público, la defensa de la privacidad, la libertad de expresión en la red, la propiedad intelectual, la cultura libre y el software libre y, por último, los movimientos sociotecnológicos (Candón Mena, 2010: 341). Pero no se tratan de revoluciones independientes y bien delimitadas, pues se entremezclan, confluyen y se integran en la realidad social.

2. La libertad y el control en el entorno web: ¿dominio o dominación?

En la actualidad se ha puesto en valor ese activo intangible que es el conocimiento llegando 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 Conocimiento (SIC). Es más, se suele entender que las TIC son precisamente el antecedente directo de la SIC, siendo la expresión fundamental de las TIC 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 democratización 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, éstos 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 la misma 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, colaboración y resolución de conflictos.

Internet se presenta como una red global con poder de procesamiento de la información y comunicación multimodal, no distinguiendo fronteras y estableciendo 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 donde “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 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), en el que revela que organismos gubernamentales y agencias implementan la censura y la vigilancia *online*. Los casos más extremos los hallamos en organismos como la Autoridad de Telecomunicaciones de 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 RT, 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 a las mismas. En este sentido, y en un intento de ofrecer trans-

parencia y confianza a sus usuarios, el gigante Facebook publica periódicamente informes sobre las solicitudes de los gobiernos y 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 semestre de 2013, y en ambos Estados Unidos es el país que más peticiones ha tramitado siendo en torno a 24.000 a lo largo del pasado año y de las cuales fueron atendidas un 80% aproximadamente (Facebook, 2014).

El profesor de la Universidad de Illinois McChesney se preguntaba en una entrevista si sería posible que el capitalismo actual imperante tolere una Internet democrática. Cuestiones como los servicios cerrados que funcionan como sustitutos de la web, los modelos de negocios basados en el intercambio comercial o uso publicitario de los datos de los usuarios, la desprotección y escasa regulación en el ámbito de la privacidad, la segmentación de los internautas o la amenaza que representa para las libertades civiles la acción conjunta de gobiernos y monopolios de la red para el control de la ciudadanía ponen de manifiesto la vulnerabilidad del ciudadano ante una web cada vez menos democrática y más controladora (Moore, 2013). En este sentido, en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2013) exigían unas garantías contra el acceso ilegítimo donde los Estados promulgasen leyes que penalicen la vigilancia ilegal de las comunicaciones por parte de agentes públicos y privados[1].

3. Metodología

Partimos de una realidad social cambiante, compleja y diversa donde el entorno web se integra radicalmente en la misma y sin el cual sería imposible describir y entender el actual tejido social. En esta investigación nos proponemos desmenuzar el ciberespacio y sus implicaciones cívicas y sociales, para lo cual se hace preciso entremezclar tres elementos que en la práctica están inevitablemente vinculados: las nuevas bases (tecno)culturales; la libertad y el control en la red; y el activismo tecnológico. Ahora bien, somos conscientes de las macrodimensiones del ciberespacio, que van mucho más allá de esa web superficial fácilmente accesible. De este modo, se convierte también en requisito imprescindible de esta investigación examinar la amplitud de la web, diseccionando cada una de sus partes y explorar sus características, tipo de usuarios, utilidades reales, etc.

En última instancia, queremos averiguar cómo son las nuevas expresiones de protesta fomentadas desde el entorno tecnológico y cuáles son sus exigencias y resultados. El activismo tecnológico (o *Hacktivismo*) nace como respuesta de una nueva sociedad que no se identifica con las estructuras de poder y de acción *offline* y que encuentra en la web un espacio de libertad y defensa de los derechos. Ahora bien, el ciberespacio tampoco escapa de la censura, la vigilancia y el control político/comercial. Ante ello, se despliega toda una web profunda cuya naturaleza es aún muy desconocida pero en la que se esconde una nebulosa digital con tantas oportunidades como amenazas.

1 Puede consultarse el texto completo de la Declaración en <https://es.necessaryandproportionate.org/text> [Consulta: 19/12/2013].

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. En nuestra investigación toman sentido especialmente el método empírico-analítico, pues nos permiten descomponer el problema propuesto como objeto de estudio en sus aspectos más básicos y fundamentales, lo cual nos posibilita aplicar métodos experimentales. En cuanto a la estructura del proceso investigador, hemos tenido en cuenta el método hipotético-deductivo, pues partimos de la observación para posteriormente plantear las hipótesis que habrán de ser verificadas. 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.

4. Las dimensiones de la web: la superficial y la *deep web*

La inmensidad de Internet es extraordinaria y muy pocos de los usuarios que navegan de forma diaria en ella son conscientes de toda esa Internet que no son capaces de alcanzar. Es preciso avanzar en una definición exacta y concreta de las dimensiones de la web que nos permita luego avanzar en los escenarios, los *modus operandi* y los contextos en los que se desarrolla el activismo tecnológico o *Hacktivismo*.

Realizaremos un recorrido ordenado y lineal en el que tomamos como punto de partida la web superficial. Ésta puede ser definida como aquella que es indexada por los motores de búsqueda tradicionales (Google, Yahoo, etc.). Esta web superficial o visible incluye todos aquellos sitios cuya información puede ser indexada por los robots de los buscadores convencionales y recuperada casi en su totalidad mediante una consulta a sus formularios de búsqueda. Se caracteriza por abarcar información no contenida en bases de datos, que es de libre acceso y cuya consulta y/o descarga no requiere la realización de un proceso de registro ni un programa específico. Ahora bien, esta web visible solo supone en torno al 5% del total de la web. Y es que el 95% restante pertenece a lo que se conoce como la *deep web* o web profunda.

Por un lado, esta web oscura está compuesta por páginas que no son indexadas a los motores de búsqueda tales como las intranets, algunas bases de datos, enciclopedias y diccionarios (como DRAE, por ejemplo), páginas y sitios web protegidos por contraseñas o documentos en formatos no indexables. “Pero la *deep web* incluye también un creciente volumen de contenidos cifrados por motivos políticos, militares, de activismo de la privacidad o puramente delictivos” (Verdú, 2014). Esa otra parte de la *deep web*, también conocida como el inframundo o las cloacas de la red, ofrece a los usuarios un “gigantesco búnker digital inexpugnable, incluso para la Policía y los servicios de inteligencia de los gobiernos” (Sánchez, 2013). Es en este espacio profundo y con la salvaguardia de no dejar rastro donde se desarrollan una serie de actividades delictivas tales como distribución de pornografía infantil y comunidades pederastas, venta de objetos robados y documentación falsa, blanqueo de dinero, compra de drogas y armas, contratación de sicarios, etc.

Algunos portales de venta de productos ilegales que podemos encontrar en la *deep web* son Agora, donde se pueden adquirir drogas; Pandora, donde encontrar armas de fuego, DNI españoles y pasaportes de todas las nacionalidades; o la ya cerrada por la FBI en octubre de 2013, Silk Road. Pero en este mercado oscuro y negro no se paga con dólares ni euros, sino con *bitcoins*, una volátil criptodivisa creada en 2009

y cuyas transacciones suelen realizarse mediante intermediarios conocidos como *escrow* o *fidecomisos* y cuya labor es retener el pago hasta que no se reciba la mercancía en el domicilio a través del correo. Además, para acceder de forma segura a estos suburbios de Internet es preciso que el usuario utilice redes encriptadas que garanticen una navegación anónima. La más famosa es Tor, un software que permite navegar de forma anónima por Internet y acceder a servidores web ocultos. El nombre alude a la cebolla, pues está formado por muchas capas que permiten que las peticiones de los usuarios vayan rebotando de un nodo a otro y saltando de país en país de manera aleatoria. De ese modo la dirección IP es sucesivamente cifrada y modificada entre cada eslabón hasta que se llega al punto de destino.

Pero Tor y la *deep web* en su conjunto no solo están siendo utilizadas desde una perspectiva delictiva relacionada con el mercado negro, las drogas, el tráfico de armas… Son defendidas por movimientos *hacktivistas* que encuentran en estos espacios las únicas vías para la lucha ciudadana en algunas países en conflicto como Siria, o lugares con férrea censura y espionaje en Internet, como China o Irán. Para la lógica *hacktivista*, los datos personales de los usuarios son hoy el nuevo petróleo para empresas privadas y organismos públicos, por lo que si no se deja rastro alguno se deja de ser rentable y, por ende, manipulable. Así lo expresaba Jacob Appelbaum, *hacker* y portavoz del proyecto Tor (Appelbaum citado en Sánchez, 2013).

Tor no debería ser considerado como algo subversivo, sino necesario. Todo el mundo debería ser capaz de hablar, leer y formarse sus propias opiniones sin ser controlado. Debería llegar un momento en el que Tor no sea considerado como una amenaza y que la sociedad confíe en él. Cuando eso pase, habremos ganado.

5. Las nuevas bases culturales: el software libre y la ética *hacker*

Para entender el nacimiento y la evolución de los movimientos activistas de corte tecnológico nos hemos de situar en la década de los 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 del mismo, como un paso previo e imprescindible para combatir el cibercontrol social (Garaizar, 2004) y batallar por la libertad del conocimiento y la justicia social. Recordemos que fue a partir de 1960 cuando las primeras compañías empezaron a privatizar sus códigos, existiendo hasta entonces un modelo de desarrollo cooperativo en el campo del software y la programación. En efecto, detrás de este giro se encuentran los intereses lucrativos y monetarios de muchas compañías que se dedicaban y dedican a comercializar estos productos:

A finales de los años 1970 y principios de los años 1980, los vendedores de computadoras y compañías de software empezaron a cobrar por licencias de software de manera rutinaria, comercializándolas como “Productos Informáticos” e imponiendo restricciones legales a los nuevos desarrollos de software, ahora vistos como activos, a través de derechos de autor, marcas registradas y contratos de arrendamiento. En 1976, Bill Gates marcó el gran cambio de era cuándo escribió su ahora famosa Carta abierta a los aficionados, mandando el mensaje de que lo que los *hackers* llaman “compartir” era, en sus palabras, “robar”[2].

2 La Carta está disponible en <http://vpabogados.files.wordpress.com/2010/09/bill_gates_letter_to_hobbyists.jpg> [Consulta: 10/08/2009].

Sin embargo, para muchos usuarios y teóricos "el acceso a los códigos de Internet, el acceso a los códigos del software que gobierna Internet, es, ha sido y sigue siendo abierto, y esto está en la base de la capacidad de innovación tecnológica constante que se ha desarrollado en Internet" (Castells, 2000: 4). La defensa de esta idea y su difusión fue lo que impulsó el nacimiento en octubre de 1985 de la Free Software Foundation (FSF) creada por Richard Stallman y otros entusiastas del software libre. Esta fundación realiza una definición concreta del significado de software libre y las libertades que supone:

«Software libre» es el software que respeta la libertad de los usuarios y la comunidad. En grandes líneas, significa que los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que este hace. Cuando los usuarios no controlan el programa, decimos que dicho programa «no es libre», o que es «privativo». Un programa que no es libre controla a los usuarios, y el programador controla el programa, con lo cual el programa resulta ser un instrumento de poder injusto.

Ya en 1985 Steven Levy defendía en su libro *Hackers. Heroes of the computer revolution* que entre estos "geniales pioneros" se imponía una filosofía común a la lógica de los ordenadores y que se basaba en la consigna de compartir, y todo ello con un fin: "mejorar las máquinas y mejorar el mundo" (Levy, citado en Tascón y Quintana, 2012:19). Y es que, "el eslogan de la clase *hacker* no es: «Obreros del mundo, uníos»; sino «Obras del mundo, liberaos»" (Wark, 2005: 17). Éstas y no otras son las consignas de la ética *hacker*. Una ética de la información esta actitud debe contener un componente cívico que, unido a un trabajo colectivo y desinteresado, puede desembocar en importantes innovaciones para la sociedad. Es lo que se conoce como *hackerismo*. No nos referimos a los denostados piratas tecnológicos. El *hackerismo* "es la cultura en la que la pasión de crear (ya sea tecnología o arte o pedagogía) es la motivación más importante, la que guía la conducta de creadoras e innovadores" (Castells, 2009:38). Es la razón de ser del software libre y la que llevó a Richard Stallman y Linus Torvalds a difundir gratuitamente el Sistema Operativo "GNU/Linux".

6. Activismo tecnológico en la era *hacker*

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.

En la actualidad, la sociedad muestra un descontento y desconfianza generalizados por las estructuras políticas y de participación ciudadana tradicionales. Los partidos políticos, sindicatos y demás asociaciones e instituciones se presentan al ciudadano 2.0 como entes anclados en una cultura pasada, regidas por rígidas jerarquías y funcionamientos internos insuficientemente transparentes. Todo ello no convence al e-ciudadano de hoy, que empieza a exigir mayor capacidad de acción y participación,

en pro de la libertad y el espíritu democrático. Internet se presenta entonces como un elemento crucial, un nuevo escenario social donde la web 2.0 ofrece la participación libre y no jerarquizada de sus usuarios, fomentando el diálogo, la colaboración y cooperación. Se tratan de estructuras descentralizadas y anti jerárquicas (Fernández Buey y Riechman, 1994) que surgen a partir de preocupaciones compartidas por una serie de personas. Internet y las redes sociales han facilitado el encuentro de esas personas con inquietudes y preocupaciones comunes. Ya no son individuos aislados en una lucha personal y absurda, ahora están amparados por una multitud anónima pero activa cuya movilización es capaz de sacudir los cimientos del sistema.

Gracias a la apropiación del entorno tecnológico, esta ciudadanía activa se desarrolla en el orbe cibernético hallando en él una herramienta tecno-cívica. 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 mediadores necesarios 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 tecno-políticas a la gente corriente" (Garaizar, 2004: 10). Los miembros de este movimiento parten de una conciencia colectiva y adquieren una actitud comprometida socialmente poniendo sus conocimientos al servicio de la ciudadanía y promoviendo políticas tales como la libertad de expresión, los derechos humanos y la ética de la información.

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" (Alexandra citado en Wikipedia, 2014). El *Hacktivismo* combina pues elementos del *hacking online* y del activismo político (Denning, 2003). Lejos del estereotipo de personas introvertidas, aisladas y exclusivamente obsesionadas con la programación y la seguridad informática, muchos *hackers* toman consciencia de las dimensiones políticas del código que escriben y se lanzan para amplificar sus efectos políticos.

El uso político que hacen los *hacktivistas* los diferencian de los *hackers* ya que, normalmente, este último es "un personaje apolítico que sólo 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 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, surgen en el seno del *Hacktivismo* una escisión que se aleja del compromiso cívico y de la que resultan los conocidos como *script kiddies*, jóvenes que intentan hacerse pasar por *hackers*, a pesar de su falta de habilidades técnicas ni 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 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 control de recursos valorados por ambos y la ruptura de los límites de compatibilidad del sistema en el que acontece la movilización (Melucci, 1999).

6.1. Dinámicas de acción

Las primeras acciones *hacktivistas* fueron los conocidos 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 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.

Tabla 1. Tipos de *Hacktivismo*, resumido por características

	Formas	**Orígenes**	**Orientación**	**Temática**	**Cuándo**
Political cracking	Desfiguración Redirección Ataques de denegación de servicios Sabotaje Información Robo	Programadores *hackers*	Fuera de la ley	Cuestiones *online* abarcando gradualmente cuestiones *offline*	Desde la década de los 90
Performative hacktivism	Parodias Sentadas	Artistas activistas	Transgresor	Cuestiones *offline*	Desde 1997
Codificación política	Desarrollo de software	Programadores *hackers*	Transgresor	Cuestiones *offline*	Desde 1999

Fuente: Samuel (2004: 101).

Las técnicas empleadas hoy día 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 causa 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 realizan 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 tal 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 y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder 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 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 anterior donde se emplean en su mayoría zombis (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 del mismo.
- 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* es 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 pretende 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.
- Etc.

6.2. Principales operaciones *hacktivistas*

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, 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 blo-

quearon las cuentas de Wikileaks, Anonymous volvió a salir en su defensa a través de una *Operation 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 convertidos con 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 clanes. Sin embargo, el 17 de julio de 2011 LulzSec celebra su tweet 1.000 y anuncia el fin de su rivalidad con Anonymous. Dos días después ambos movimientos inician 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 ecológica y comprometida con el medio ambiente organizó la Operación Green Rights, especialmente tras el tsunami y 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 de “do-ocracy” (estructura flexible en la que los individuos se autoseleccionan las tareas a llevar a cabo), restableció parcialmente el acceso a la web en Egipto, repitiendo la misma operación en Libia en febrero de 2011.

En el año 2012 se desarrolló la Operación Represalia donde algunos colectivos *hacktivistas*, Anonymous entre otros, se enzarzarían en una lucha como represalia al cierre de Megaupload y el apoyo de la compañía discográfica a la ley SOPA.

Aquí en España, la polémica Ley de Economía Sostenible, conocida como la Ley Sinde, referente a los derechos de propiedad intelectual y las descargas de Internet, ha sido también objeto de Anonymous. El conocimiento de la Ley de Economía Sostenible, promovida por la ministra de Cultura, Ángeles González-Sinde, provocó una revuelta en Internet sin precedentes entre los usuarios, entre los que se encontraba Anonymous. Como respuesta, se organizó un ataque coordinado contra los sitios en Internet de la SGAE y del Ministerio de Cultura. Ambas webs tuvieron cortes importantes en el servicio, como consecuencia de los ataques DdoS iniciados por el grupo.

Los ataques a dichas webs seguirían posteriormente en fechas puntuales, como la del 20 de diciembre de 2010, día en el que se realizó la votación de la Ley Sinde en el Congreso, y que afectaría a otras webs como la oficial del Congreso de los Diputados y la de los partidos PSOE, PP, PNV y CiU. El 16 de enero de 2011, día de su aprobación en el Senado, volvieron a la carga colapsando, además, las web del Senado Español y de la Embajada de EEUU. El 29 de enero de 2012, Anonymous publica en la red datos personales de autoridades políticas partidarios de la mencionada ley, entre los que se encuentran la ex ministra Ángeles González-Sinde, el ministro de

cultura José Ignacio Wert, así como de artistas y productoras de cine. Poco después, el 20 de febrero de ese mismo año, con motivo de los Premios Goya, se vuelven a filtrar datos personales de los miembros de la Academia, como señal de protesta ante la Ley Sinde.

7. Conclusiones

Esta investigación desarrolla un recorrido analítico descriptivo de la situación actual de los movimientos cívicos de componente tecnológico, así como las bases culturales y sociales en las que se sustentan. El desarrollo tecnológico así como el avance de Internet ha marcado un punto de inflexión en el propio devenir ciudadano y sus dinámicas de actuación. La ética *hacker* con sus consignas de transparencia y colaboración, unida a la voluntad de desarrollo de espacios colaborativos y de conocimiento compartido contrastan las estructuras de control, censura y cibervigilancia que intentan imponer organismos públicos y/o privados.

En entorno *online* es entendido como un espacio de desarrollo democrático e igualitario donde la libertad de expresión y de circulación de ideas debe tener su máxima expresión. Sin embargo, cada día el usuario se siente más monitoreado y su privacidad más vulnerada. De este modo, en Internet encontramos espacios que pretenden escapar a ese control y en los que los usuarios gocen de una total libertad. Ha quedado demostrado a lo largo de la investigación que esta dimensión oscura y oculta de la web alberga delincuentes, pederastas, traficantes y un sinfín de actividades delictivas. Pero también resultan los únicos espacios válidos donde ejercer la lucha ciudadana en países no democrático y con férreos sistemas de censura.

Desde hace tiempo el entorno web se ha convertido en una importante herramienta para ejercer y desarrollar el activismo social. Han surgido grupos que entienden que el alcance de la tecnología va más allá de 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 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 las mismas 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 estos actos y unos detractores que se oponen a los mismos.

8. Referencias

Aceros, J. C. (2006). *Jóvenes, Hacktivismo y Sociedad de la Información.* Barcelona: Universidad de Barcelona. Recuperado de http://www20.gencat.cat/docs/Joventut/Documents/Arxiu/OCJ/InformeAceros.pdf.

Bustamante Donas, J. (2001). Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. R*evista Iberoamericana*

de Ciencia, Tecnología e Innovación, 1. Recuperado de http://www.oei.es/revistactsi/numero1/bustamante.htm.

Candón Mena, J. y Ortega Gutiérrez, F. (2011). *Internet en movimiento.* Madrid: Universidad Complutense de Madrid.

Castells, M. (2000). *Internet y la Sociedad en Red. Lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement.* Barcelona: Universidad Oberta de Cataluña.

Castells, M. (2001). Internet: ¿una arquitectura de libertad? Libre comunicación y control del poder. Recuperado de http://www.uoc.edu/web/esp/launiversidad/inaugural01/internet_arq.html.

Castells, M. (2009). *Acto de investidura como Doctor Honoris Causa de la Universidad de Sevilla del profesor Dr. Manuel Castells Oliván.* Sevilla: Secretariado de Publicaciones de la Universidad de Sevilla.

Denning, D. E. (2003). Activismo, Hacktivismo y Ciberterrorismo: Internet como instrumento de influencia en política exterior. En Arquilla, John y Ronfeldt, David (2001). *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político.* Versión castellana de Francisco Muñoz de Bustillo. Madrid: Alianza Editorial.

Dron, J. (2007). Designing the Undesignable: Social Software and Control. *Educational Technology & Society,* 10 (3), 60-71.

Echeverría, J. (1999): *Los señores del aire: Telépolis y el Tercer Entorno.* Barcelona: Ediciones Destino.

Facebook (2013). Informe de solicitudes de gobiernos. Recuperado de https://www.facebook.com/about/government_requests.

Facebook (2014). Informe sobre solicitudes gubernamentales. Recuperado de https://govtrequests.facebook.com/.

Fernández Buey, F. y Reichman, J. (1994). *Redes que dan libertad. Introducción a los nuevos movimientos sociales.* Barcelona: Paidós Ibérica.

Garaizar Sagarminaga, P. (2004). *El Software Libre como herramienta de Hacktivismo contra el cibercontrol social.* Ediciones Simbióticas. Recuperado de http://www.edicionessimbioticas.info/IMG/pdf/ACTIVISMO_Y_SOF_LIBRE.pdf.

Lobo, J. L. (2013). ¿Nos espía Rajoy? El Gobierno escruta sin control judicial llamadas y correos electrónicos. *El Confidencial,* 5 de julio. Recuperado de http://www.elconfidencial.com/espana/2013/07/05/nos-espia-rajoy-el-gobierno-escruta-sin-control-judicial-llamadas-y-correos-electronicos-124355.

Meer, H. (2011). Lecciones de Anonymous sobre la guerra cibernética. *Rebelión,* 12 de marzo. Recuperado de http://www.rebelion.org/noticia.php?id=124068.

Melucci, A. (1999). *Acción colectiva, vida cotidiana y democracia.* México: El Colegio de México, Centro de Estudios Sociológicos. PMid: 10432982.

Moore, A. E. (2013). “Can Capitalism Tolerate a Democratic Internet? An Interview With Media Expert Robert McChesney”. *Truthout*, 3 de abril. Recuperado de http://truth-out.org/opinion/item/15516-can-capitalism-tolerate-a-democratic-internet-an-interview-with-media-expert-robert-mcchesney.

Orihuela, J. L. (2005). Apuntes sobre redes sociales. Recuperado de http://www.ecuaderno.com/2005/07/19/apuntes-sobre-redes-sociales.

Paget, F. (2012). Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas. McAfee Labs. Recuperado de http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf.

Reporteros Sin Fronteras (2014). Enemigos de Internet. Recuperado de http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/.

Samuel, A. (2004). *Hacktivismo y el futuro de la participación política.* Tesis Doctoral, Massachusetts: Harvard University. Recuperado de http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-chapter2.pdf.

Sánchez, C. M. (2013). Bienvenidos a la web oculta. *XLSemanal,* 6 de octubre, pp. 31-38.

Tascón, M. y Quintana, Y. (2012). *Ciberactivismo. Las nuevas revoluciones de las multitudes conectadas.* Madrid: Catarata.

Verdú, D. (2014). Lo que Google no ve. *El País,* 7 de junio. Recuperado de http://sociedad.elpais.com/sociedad/2014/06/06/actualidad/1402082139_266819.html.

Vicente, L. (2004). ¿Movimientos sociales en la Red? Los hacktivistas. *El Cotidiano,* 20 (126). Recuperado de http://www.redalyc.org/pdf/325/32512615.pdf.

Wark, M. (2005). *Un manifiesto hacker.* Barcelona: Alpha Decay.

Wikipedia (2014). Hacktivismo. Recuperado de http://es.wikipedia.org/wiki/Hacktivismo.