Universidad de San Andrés

Departamento de Derecho

Tesis de Grado - Carrera de abogacía

El tratamiento jurídico del hacktivismo: ¿Una conducta criminal o una forma legítima de protesta y expresión?

Alejandro Comesaña

Legajo: 22296

Mentor: Pablo Palazzi

Buenos Aires, Argentina. 2017

Índice

Abstract

El desarrollo tecnológico ha dado lugar a nuevos canales de expresión y protesta que se valen de las plataformas digitales para transmitir un mensaje social y político. Este fenómeno llamado hacktivismo implica la unión entre el uso de herramientas tecnológicas y el activismo tradicionalmente entendido. Si bien muchas de las herramientas utilizadas por el movimiento pueden tener efectos y fines dañinos a la propiedad privada e intelectual, existen otros métodos que se asimilan a actos de desobediencia civil y protesta, y por lo tanto dichas acciones deberían contar con un cierto grado de protección jurídica en consonancia con el Articulo 19 del Pacto Internacional de Derechos Civiles y Políticos y la Declaración Universal de Derechos Humanos.

El marco jurídico internacional actual que no contempla ninguna distinción entre el hacktivismo con fines políticos y el hacking con fines personales, representa una violación a la libertad de expresión y el derecho a la protesta protegido convencionalmente. Si bien es necesario un marco jurídico que sancione y prevenga actos de hacking y ciertos actos de hacktivismo cuyas consecuencias vulneran grave e inequívocamente el derecho a la propiedad de terceros, las normas actuales deben ser actualizadas a modo de que no se castigue de manera desproporcionada el uso tecnológico con fines activistas.

Primer Capítulo: La era digital y las nuevas formas de protesta

Introducción

Históricamente, las protestas públicas llevadas a cabo por individuos y grupos activistas han cumplido un rol fundamental en el desarrollo civil, político, económico y cultural de los estados. Su papel como una forma de expresión y manifestación de descontento frente a las autoridades e instituciones ha sido un pilar fundamental de las democracias representativas, e innegablemente ha contribuido a generar avances sociales en materia de protección de derechos humanos y libertades civiles.

La eclosión de la era digital, marcada por los revolucionarios cambios introducidos por el concepto de internet, ha transformado completamente la relación humana con la tecnología, modificando las formas de interacción social, los medios de acceso a la información, las formas de participación política, y las vías mediante las cuales los individuos expresan sus ideas y preocupaciones. Debido a las enormes oportunidades y desafíos presentados por la expansión de internet, legisladores alrededor del mundo han tenido que hacerle frente a las problemáticas emergentes de esta nueva plataforma, demostrando la dificultad de mantener un sistema jurídico actualizado frente a los incesantes cambios y avances tecnológicos.

El hacking y los delitos informáticos han sido la primer amenaza que a partir de la década de 1980 despertaron la necesidad de aplicar normas regulatorias al uso y abuso de herramientas tecnológicas e internet. Ya para finales de esa década, comenzó la proliferación de un conjunto de actividades relacionadas con el hacking, pero que hacían énfasis en su utilización como medio de denuncia de actividades relacionadas con la proliferación nuclear, combinando el humor y las herramientas tecnológicas con el fin de transmitir un mensaje político, social, y ambiental. Un nuevo término sería acuñado para identificar este tipo de actividades*: Hacktivismo,* un término que para la primera década del siglo XXI, se convertiría en un fenómeno cultural, tecnológico, social y político, que pondría en jaque los marcos jurídicos existentes, y las concepciones tradicionales de protesta.

Este trabajo se enfocará en el debate y controversia que gira en torno al tratamiento jurídico del hacktivismo: ¿Debería ser considerada como una legítima forma de expresión y de protesta? ¿O no es más que un intento de atribuirle un valor moral a una actividad criminal? ¿Es legítimo y eficiente el sistema jurídico actual que equipara al hacktivismo con el ciberterrorismo y los delitos informáticos, o acaso este sistema implica una persecución penal que viola convenciones protectoras de derechos fundamentales? Este trabajo tendrá como objetivo dilucidar estas cuestiones con el fin de facilitar la compresión del hacktivismo como fenómeno tecnológico y social, y comprender la necesidad de un marco jurídico actualizado que por un lado asegure el respeto de la propiedad privada en el ámbito digital, y por el otro reconozca los beneficios y aspectos del hacktivismo que contribuyen a una sociedad más transparente, informada y participativa.

Este fenómeno tecnológico ha demostrado por un lado el enorme poder de las herramientas informáticas como medio de protesta y su capacidad para fomentar la participación ciudadana en el debate de la agenda pública, y por el otro, los grandes daños económicos que pueden generar tanto a corporaciones como estados, representando una verdadera amenaza a la propiedad privada y el derecho a la privacidad. Las acciones de grupos hacktivistas prominentes como Wikileaks y Anonymous han despertado un extenso debate académico y jurídico sobre cómo deberían encuadrarse este tipo de acciones frente al derecho internacional. En un extremo, se encuentra la posición que reclama la legitimación y protección legal del hacktivismo en todas sus variantes, planteándolo como una forma auténtica de activismo político, análoga a los métodos de protesta tradicionales y la desobediencia civil, siendo por lo tanto una actividad protegida por tratados y convenciones internacionales sobre derechos humanos. En su contra parte, se encuentra la postura que ve en este fenómeno un medio mediante el cual un grupo reducido de criminales es capaz de vulnerar el derecho a la privacidad y la propiedad privada, escondiéndose bajo el velo de anonimidad e impunidad que provee internet, y por lo tanto debe ser encuadrado legalmente como un delito informático, al igual que el hacking y sus variantes.

En primer lugar, uno de los objetivos de este trabajo será brindar un panorama claro sobre las diferentes formas y métodos que se consideran parte de la actividad hacktivista, y

como cada una tiene efectos y motivaciones que varían según el caso particular. Una visión clara de estos conceptos facilita la comprensión de las contraposiciones legales en juego, y permite ponderar la idoneidad y legitimidad de normas restrictivas. Debido a la naturaleza del conflicto en cuestión, el hacktivismo no puede ser observado desde un punto de vista local, sino que debe contemplarse desde una perspectiva transnacional. Por lo tanto, este trabajo contemplará las normas internacionales existentes, y se enfocara en mayor medida, en las normas vigentes y los casos resueltos en estados occidentales, sobre todo en los Estados Unidos, ya que la mayoría de los casos más trascendentales sobre el tema se han debatido en estos territorios.

En segundo lugar, intentaré ilustrar cómo la actual carencia de regímenes legales locales y convenios internacionales que contemplen al hacktivismo de manera independiente del hacking y el ciberterrorismo, ha resultado en la persecución y aplicación de lo que muchos juristas y activistas consideran penas desproporcionadas, criminalizando acciones de manera inconsistente e incompatible con el libre ejercicio de derechos civiles. Esta posición no implica considerar que todas las acciones cometidas bajo este concepto representan una legítima forma de expresión, ni tampoco adoptar la postura extrema que considera que internet debe ser un espacio carente de regulaciones, libre de cualquier limitación jurídica. La libertad de expresarse y protestar, como todos los derechos, debe estar sujeto a ciertas limitaciones que eviten su abuso ilegítimo.

Según, Steven Chabinsky, director del departamento de ciber seguridad del FBI, los delitos informáticos y el ciberterrorismo representan una de las amenazas existenciales más serias contra la infraestructura y la seguridad nacional de los Estados Unidos[1]. Es evidente la necesidad de marcos jurídicos que mitiguen los riesgos que presenta el abuso de las herramientas informáticas a la propiedad y la privacidad, pero sostengo que dichas normas deben contemplar el hecho de que el desarrollo tecnológico ha dado lugar a nuevas formas de activismo que no pueden ser comprendidas en un sentido tradicional, ya que no pretenden articularse a las instituciones políticas existentes.[2]

[1] Chabinsky, Steven. GovSec/FOSE Conference. 23/4/2010
[2] Burgos Pino, Edixela Karitza. El hacktivismo: Entre la participación política y la tácticas de subversión digital. p.21

El fenómeno del hacktivismo debería ser contemplado independientemente del hacking, teniendo en cuenta el contexto en el que estas actividades se llevan a cabo. Esto facilitaría, por un lado, evitar la criminalización de conductas que pueden contribuir en la creación de sociedades más transparentes y ciudadanos más activos e informados, y por el otro, proteger la propiedad privada y la privacidad, criminalizando actos que a pesar de ser considerados hacktivistas, generan daños y riesgos que escapan la protección brindada por los instrumentos convencionales y el derecho local.

Conceptualización de la actividad hacktivista y sus diferencias con términos similares

Para abordar un análisis claro de las actividades que implican un acto de hacktivismo propiamente dicho, es necesaria su definición conceptual a modo de poder diferenciarlo con otros términos similares originados del campo informático. Las confusiones más comunes son las que se dan entre los conceptos de *hacktivismo*, *hacking*, *ciber terrorismo*, y *ciber activismo*. Si bien todos estos términos implican el uso de herramientas digitales, sus efectos, motivaciones, métodos, y objetivos son radicalmente distintos, y por lo tanto, un ordenamiento jurídico eficiente debería tener en cuenta dichas diferencias.

Los orígenes del hacking se remontan a la década de los 60, donde internet no formaba parte de la realidad informática, y la manipulación digital no era más que una forma de experimentación con el fin de desarrollar tecnologías computacionales más avanzadas. Para la década de los 80, el término se convirtió en una sub cultura con una serie de principios éticos fundados en la noción de que toda la información en internet debería ser de libre acceso, y no deberían existir barreras burocráticas que dificulten de ninguna manera dicho acceso[3]. Estos principios éticos además fomentaban la descentralización del conocimiento, el escepticismo hacia toda figura de autoridad y la emancipación de la tecnología, cuyo libre uso y desarrollo resultaría en sociedades más democráticas.

En la actualidad, las actividades relacionadas con el hacking son entendidas popularmente como el uso de conocimientos informáticos con fines fraudulentos, pero esta

[3] Levy, Steve. "Hackers: Heroes of the Computer Revolution". 1984

definición simplificada no resulta suficiente para comprender las variantes del fenómeno en su totalidad. Este se puede manifestar de diversas maneras y configurar diferentes delitos, dentro de los cuales se encuentran el robo de identidad, el fraude, el espionaje comercial y otros tipos de actividades que se caracterizan principalmente por estar motivadas en el interés económico personal del hacker. Estos son los delitos informáticos tradicionales, para los cuales la mayoría de los estados occidentales han configurado regímenes penales para su sanción.

Por otro lado, existe el concepto del ciber terrorismo, que representa un extremo del espectro, pudiendo ser definido a partir de sus similitudes con los objetivos típicos de las actividades terroristas. Este involucra acciones que implican el uso informático para generar pánico en poblaciones civiles, muchas veces traducido en la creación de un riesgo en la vida de personas, como lo sería interferir con equipos de navegación de vuelos internacionales y aeropuertos, o irrumpir en los servidores de un hospital.

Por su parte, el hacktivismo es un concepto que engloba diversas conductas, algunas con consecuencias económicas leves o nulas, y otras más disruptivas que pueden llegar a generar daños económicos graves. El hacktivismo comparte los mismos principios éticos que el hacking, por lo que entra en conflicto directo con la noción comercial e industrial que desea la regulación y el control sobre internet.[4] Es por este motivo que el hacktivismo ha sido vilificado por los estados y los medios de comunicación masivos, siendo representado como una amenaza para la sociedad y la seguridad nacional. Dado que la mayoría de las manifestaciones hacktivistas han tenido como objetivo órganos estatales y corporaciones, mediáticamente se lo ha presentado como un sinónimo de ciber terrorismo, a pesar de que dichos usos tecnológicos con el único fin de generar daños físicos y patrimoniales hayan sido condenados abiertamente por la comunidad hacktivista.[5]

En el sentido más abarcador, como su nombre lo indica, el hacktivismo es aquella actividad que se vale de las herramientas informáticas para realizar un acto activista. En otras palabras, involucra el uso de conocimientos informáticos con el propósito de generar

[4] Manion and Goodrum, 2000.
[5] Mikhaylova, Galina, THE "ANONYMOUS" MOVEMENT: HACKTIVISM AS AN EMERGING FORM OF POLITICAL PARTICIPATION, 2014.

cambios políticos y sociales, transmitiendo un mensaje ideológico y de esa manera contribuir a generar consciencia, situando determinado tema en la agenda pública. Esta definición del concepto es compartida por autores como Denning, Milone, y Jordan,[6] cuyas interpretaciones permiten resumir al término como una manifestación activista políticamente motivada, llevada a cabo por actores no estatales con el fin de expresar un descontento o llamar la atención a cierto tema en particular, valiéndose de herramientas informáticas ilegales o legalmente ambiguas. Este tipo de ataques no suele estar dirigido a la población civil, y dependiendo de su modalidad, involucrará acciones pacíficas de mera exposición visual de descontento y protesta, a ataques más organizados y disruptivos, con el propósito de, como por ejemplo, hacer pública información confidencial del Estado y de entes privados o bloquear e interrumpir el acceso a determinados sitios.

Una definición de este tipo permite separar al hacktivismo del hacking y el ciberterrorismo, haciendo énfasis en la motivación política que lo impulsa y los fines no violentos que persigue, contemplando al mismo tiempo el uso de herramientas de ilegales o de legalidad ambigua, que separa al hacktivismo del mero activismo online.

De la misma manera que la tecnología evoluciona, los métodos y herramientas utilizados por los hacktivistas se adaptan y moldean de acuerdo a los avances informáticos y los objetivos buscados. Este avance no sólo da lugar a métodos más efectivos de comunicación, sino que también da origen a herramientas informáticas más disruptivas y que pueden generar daños mucho mayores. Debido al amplio espectro conceptual que abarca la idea de hacktivismo, y debido a la variedad de acciones y herramientas utilizadas para alcanzar los fines que se plantean, analizar la legitimidad y legalidad de estas acciones no es una tarea fácil de realizar. Para ello resulta útil y necesario comprender los modos y los efectos que generan las diferentes herramientas utilizadas por los hacktivistas, ya que algunas pueden compararse con los métodos tradicionales de protesta y las inconveniencias que estas implican, pero otras pueden resultar más difíciles de defender desde este punto de vista, dado el nivel de disrupción y daños que generan.

[6] Jordan, Tim, and Paul A. Taylor. *Hacktivism and cyberwars: rebels with a cause?*. 2004.

Modalidades de hacktivismo y sus efectos particulares

Las diferentes herramientas utilizadas por el movimiento hacktivista responden a diferentes posturas políticas y diferentes tácticas tenidas en cuenta con el fin de transmitir efectivamente el mensaje deseado[7]. Estas modalidades son variadas en cuanto a sus efectos, sus grados de disrupción, y por lo tanto, sus grados de legitimidad como una forma de protesta y expresión. Si bien existen varios tipos de hacktivismo, limitaré su análisis a los métodos más relevantes y comúnmente utilizados por quienes plantean la necesidad de una actualización normativa que brinde protección jurídica a este concepto.

Las manifestaciones más relevantes de hacktivismo suelen resumirse en 5 tipos de acción[8]. Estos son el "*Denial of service attack*" (Ataque de denegación de servicio o DoS)", los "*Site defacements*" (considerado como graffitti digital), los "*Site redirects*", "*Visual sit-ins*" y el robo de información (Doxing). Resulta necesario comprender y delimitar cada uno de estos comportamientos ya que sus efectos varían drásticamente, siendo algunos más disruptivos y dañinos que otros, y por lo tanto, poniendo en cuestión hasta qué punto podemos estar hablando de un derecho a expresarse libremente. Además resulta pertinente aclarar que estos no son los únicos modos que podrían clasificarse dentro de la categoría en cuestión, y que con el veloz progreso tecnológico en materia informática, estos métodos están condenados a variar y evolucionar con el tiempo.

Denial of service (DOS) y Distributed denial of service (DDOS)

Estas herramientas tienen como objetivo saturar un servidor o sistema determinado de modo que su funcionamiento se vea comprometido y sus usuarios tengan dificultades en acceder a un sitio web por un tiempo indefinido. El ataque de denegación de servicio (DOS) se vale de una sobrecarga de los servidores que genera un excesivo tráfico de información que culmina en que el sistema o servidor no pueda operar como lo haría normalmente, y por lo tanto los usuarios legítimos del sitio no pueden acceder al contenido.

Un ataque de denegación de servicio distribuido (DDOS) funciona de la misma manera, diferenciándose del primero por valerse de una red de múltiples computadoras

[7] Samuel, Hacktivism and the future of political participation, pg 205.
[8] Hampson. A new breed of protest Pag. 8

para saturar el server host y como resultado, obtener un bloqueo temporal del sitio. Los ataques DDOS implican a diferentes regímenes jurídicos, ya que generalmente el grupo que inicia el ataque está situado en el país A, se vale de computadoras y servers ubicados en los países, B, C y D, y ataca un server ubicado en el país E. Esto dificulta la persecución penal de los perpetradores, y convierte su investigación en una tarea sumamente laboriosa y costosa. Además, el desarrollo de software libre ha convertido al DDOS en una herramienta accesible incluso para quienes no poseen un profundo conocimiento informático. Un ejemplo de ello es el *LowOrbit Ion Cannon*, un software de acceso gratuito diseñado por hackers, creado para que aquellos que quieran participar de un ataque para demostrar su apoyo con una determinada causa, puedan hacerlo ofreciendo los recursos de sus computadoras.

La utilización de esta herramienta ha aumentado exponencialmente en los últimos años, convirtiéndose en uno de los métodos más comunes, no solo por su efectividad, sino por su creciente accesibilidad participativa para los ciudadanos promedio sin conocimientos ni experticia informática. Algunos ejemplos recientes de DDOS relacionados con actividades hacktivistas fueron los ataques realizados por el grupo Anonymous en el marco las olimpiadas a ser realizadas en Brasil. Este grupo hacktivista se unió a la causa de los manifestantes que protestaban en contra del evento y las autoridades gubernamentales, atacando múltiples sitios estatales, dejándolos fuera de uso temporalmente, y haciendo publica información personal y financiera de diversas asociaciones deportivas relacionadas con el evento.

Site defacements

Este método involucra el acceso a un servidor web para alterar el diseño y contenido visual de determinada página. Se lo considera como un "graffiti digital", en donde se utiliza el hacking para tener acceso a un sitio, y modificar visualmente su estructura con el fin de transmitir un mensaje determinado. Este mensaje suele ser una crítica a las actividades de una organización privada o estatal.

Los casos de site defacements fueron los primeros en captar la atención mediática a principios del siglo 21, y su uso ha aumentado notablemente. A pesar de que esta

herramienta es capaz de generar daños económicos debido al impacto en la imagen pública de una empresa, son considerados de los métodos menos dañinos de hacktivismo, y por lo tanto, utilizado por aquellos quienes desean expresar su mensaje sin incurrir en métodos más disruptivos como los ataques DDOS, que además suelen ser investigados más profundamente.

Robo de información (Doxing)

Como su nombre lo indica, este método implica el acceso no autorizado a un servidor privado con el fin de extraer información privada o confidencial. Este método es considerado una de las facetas más amenazantes del hacktivismo, que parece ignorar todo tipo de norma referente a los derechos de la privacidad y la propiedad privada.

Según un reporte realizado por la empresa Verizon, solo en 2011, individuos y organizaciones hacktivistas lograron extraer 174 millones de archivos extraídos de fuentes de datos tanto de agencias gubernamentales como de empresas del sector privado.[9] En la argumentación a favor de la legitimación del hacktivismo, se hace referencia a los casos en los que la información es robada debido a su carácter de interés público y el derecho de la ciudadanía a informarse. Un ejemplo de esta instancia, fue lo acontecido en 2009 cuando Wikileaks publicó documentación del banco Islandés Kaupthing Bank, ligando a la organización a una serie de escándalos financieros. Los documentos y el descontento que generaron las noticias llevaron a investigaciones formales que desembocaron en la convicción de 4 ejecutivos del banco, sentenciados por incurrir en la manipulación del mercado en beneficio propio. En este caso se argumenta que el robo de la información cumplió un propósito de interés público, logrando generar un cambio positivo social mediante la convicción de un grupo de criminales. A pesar de que este método sea uno de los menos ambiguos a la hora de analizar su legalidad, suele ser aceptado dentro de la comunidad hacktivista.

El problema de buscar la legitimación jurídica de casos de este tipo estaría en la dificultad en argumentar a favor del robo de información, incluso en el caso de tratarse de información de interés público. De la misma manera que entrar en las oficinas de una

[9] BBC. Data theft: Hacktivists 'steal more than criminals'. Url: http://www.bbc.com/news/technology-17428618

empresa y robar documentos representa una clara violación de la ley, el hecho de que este robo de información se de en el plano digital no debería tener un tratamiento legal diferente. Nuevamente estamos frente a la contraposición del derecho a manifestarse en pos de un bien común, contra el derecho a la privacidad y la propiedad. Diera la impresión que en casos de este tipo, el único tipo de discusión que cabe al respecto sería en la determinación de la severidad de las penas aplicables. ¿Debería penarse de la misma manera robar información con el fin de exponer una conducta criminal por parte de una organización, que robar la información bancaria de un individuo con el fin de enriquecerse? En la actualidad, ambos casos son similares ante la ley.

Virtual Sit-in (Sentada Virtual)

Esta es considerada una forma de desobediencia civil similar a la estrategia política adoptada por los movimientos de derechos civiles de la década de los 60, caracterizada por la ocupación de un espacio físico para promover determinado mensaje. Esta sería su variante digital, donde aquellos partícipes intentan acceder a un sitio de manera simultánea y repetida con el fin de enlentecer o interrumpir el funcionamiento adecuado del sitio web.

Este método opera bajo el mismo concepto que un ataque DDOS, pero al valerse únicamente de individuos particulares y no de herramientas como los botnets voluntarios o involuntarios, es considerada una de las formas de hacktivismo menos intrusivas y con más posibilidades de ser legitimada legalmente como un método de protesta. Las sentadas virtuales más grandes han sido las organizadas por los grupos activistas Electronic Disturbance Theater, y Electrohippies, las cuales contribuyeron a la difusión del concepto del hacktivismo como una manifestación artística y una forma de protesta no violenta, en el marco de las masivas manifestaciones anti-globalización de fines de los noventa.

Site redirect

Este método involucra el acceso no autorizado a un servidor para que los usuarios y consumidores de este sean redirigidos a un sitio alternativo[10]. De esta manera se toma control del sitio atacado, y se lo suplanta con otro diseñado para criticarlo

[10] Samuel, P.10

Segundo Capítulo: Un orden en la anarquía digital

El marco jurídico existente

Planteado el marco conceptual y práctico en el que opera el hacktivismo, resulta evidente la compleja variedad de situaciones y bienes jurídicos que pueden ser afectados por estas actividades. Además, en consideración del carácter internacional en el que la mayoría de estos casos se desenvuelven, la materia se complejiza aún más en cuestión de jurisdicciones y el derecho aplicable en cada caso. Debido a este factor, es clara la necesidad de un orden jurídico que facilite la cooperación entre las naciones para la identificación y eventual persecución penal.

Hay que resaltar el hecho de que no existe en la actualidad ningún acuerdo ni convenio que trate específicamente los casos que podrían encuadrarse bajo el concepto de hacktivismo. Todos los intentos legislativos han hecho foco en el hacking y los delitos informáticos, y debido a la similitud en las herramientas utilizadas, estas normas han sido aplicadas para juzgar los casos encuadrables bajo la idea de un acto hacktivista.

Convenio de Budapest sobre ciberdelincuencia

El primer y único esfuerzo internacional para tratar los crecientes y potenciales riesgos de los delitos cibernéticos y el ciberterrorismo fue el Convenio sobre Cibercriminalidad, conocido también como el Convenio de Budapest sobre ciberdelincuencia[11]. Esta convención, entrada en vigor en 2004 y ratificada por 37 Estados,

[11] Council of Europe. Convention on Cybercrime. 2001. Url: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

establece en su preámbulo como objetivo principal aumentar la cooperación entre las naciones parte, armonizando sus respectivas leyes internas con los fines convencionales, a modo de facilitar las tareas de investigación y persecución de las conductas tipificadas como delitos informáticos.

La norma hace énfasis particular en temas relacionados con la violación de derechos de copyright, el fraude, la pornografía infantil, y el acceso no autorizado a redes y sistemas privados.

Si bien esta convención hizo foco en los actos de hacking propiamente dichos, sus disposiciones pueden extenderse a la mayoría de los actos que entrarían dentro de la categoría conceptual del hacktivismo. Dentro de ellas, podemos mencionar el Art.2, que criminaliza el acceso ilegal a servidores y sistemas privados y públicos, evadiendo medidas de seguridad o explotando las debilidades del sistema. Dichas vulneraciones, según el Art.3, deben estar motivadas en la obtención de información confidencial con fines deshonestos. También se hace mención en el Art.5 a la intercepción de información privada y a la destrucción, alteración, o supresión de datos con el fin de crear daños y entorpecer el funcionamiento de servidores privados. Por último, el Art.6 se refiere a la distribución de programas y herramientas que faciliten la realización de acciones mencionadas en los artículos anteriores. Si bien la enumeración de las conductas punibles no es exhaustiva, los artículos establecen de manera general y abarcadora que estas se extenderán a todas las ofensas criminales cometidas por medio de sistemas informáticos.

El Art 15 de la convención establece de manera clara los límites del alcance de las disposiciones adoptadas por los estados firmantes. Este artículo plantea que los procedimientos adoptados deben estar sujetos a las protecciones brindadas por tratados internacionales referentes los derechos humanos y las libertades civiles de los ciudadanos. Se hace alusión directa a la Convención Europea de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, y cualquier otro pacto referente a derechos humanos. Además, en este artículo al igual que en el preámbulo de la convención, se menciona como principio rector el principio de proporcionalidad, y la necesidad de alcanzar un balance entre los intereses de la acción penal y el respeto a los derechos fundamentales, sobre todo aquellos que reafirman el derecho la libertad de expresión y

opinión sin interferencia, incluyendo la libertad de buscar, difundir y recibir información e ideas de toda índole.

Podemos ver cómo a partir de la interpretación de la Convención, todos las herramientas y actividades hacktivistas referidas en el primer capítulo representan un comportamiento criminal frente al derecho internacional, ya que lo que se tiene en cuenta no son las motivaciones de un acto, sino el acto en sí y las herramientas utilizadas para llevarlo a cabo. El preámbulo y el Art.15 serían las únicas disposiciones que dejarían margen para una interpretación protectora del hacktivismo, ya que hace énfasis en la idea de satisfacer un balance entre los intereses privados y el derecho a la libertad de expresión entendido de manera general.

Ahora bien, el Convenio de Ciberdelincuencia no ha tenido peso significante en la resolución de casos sobre hacktivismo, para los cuales se ha aplicado en su totalidad normas de derecho interno. La redacción actual del convenio evidencia como en el plano internacional no existe distinción jurídica entre los conceptos de hacking, ciberterrorismo y hacktivismo, por lo que se deja poco lugar para el debate sobre el uso tecnológico con fines activistas.

El tratamiento jurídico del hacktivismo en los Estados Unidos: The Computer Fraud and Abuse Act (CFAA)

Considero que esta norma estadounidense es de suma importancia para comprender la situación legal actual del hacktivismo, ya que si bien la CFAA fue creada con el propósito de encuadrar legalmente al hacking propiamente dicho, algunos de los casos judiciales más trascendentales sobre su variante activista han implicado la interpretación de esta norma. Además, esta ley no sólo es aplicable a todas las computadoras ubicadas en el territorio estadounidense, sino que puede extenderse a otras naciones *"(...) incluyendo a cualquier computadora ubicada fuera de los Estados Unidos que sea utilizada de manera que afecte el comercio o las comunicaciones de los Estados Unidos*" [12]

[12] 18 U.S.C. § 1030(e)(2)

Esta ley fue creada en 1984, como resultado de la creciente popularidad y preocupación que presentaba en ese momento el nuevo y aún poco comprendido fenómeno del hacking. Bajo el temor de que estas herramientas fuesen utilizadas con propósitos terroristas, logrando acceder al arsenal nuclear estadounidense, o generando daños económicos mediante el robo de información, la respuesta legislativa fue la CFAA.

El énfasis de esta norma se fundó sobre la idea de la criminalización de la conducta tipificada como "*acceso no autorizado*". Esta disposición enumera siete tipos de actividades criminales: obtener información sobre asuntos de seguridad nacional; comprometer la confidencialidad; acceder ilegítimamente a un sistema gubernamental; acceder ilegítimamente con fines fraudulentos; generar daños a una computadora o información; traficar contraseñas; y amenazar con dañar una computadora o sistema.

La CFAA ha sido criticada duramente por parte de juristas, activistas, periodistas y especialistas informáticos. En primer lugar, estas críticas han hecho foco en la vaguedad del término "*acceso no autorizado*" y "*computadora protegida*"[13], cuya falta de definición clara ha otorgado una discreción interpretativa sobre qué ha resultado en un uso abusivo de la norma.[14]

El Departamento de Justicia Estadounidense ha sostenido que una persona estaría en violación de la CFAA simplemente por el hecho de no cumplir los términos de servicio de un acuerdo online, como por ejemplo, no utilizar un nombre verdadero en la inscripción de un usuario de LinkedIn o Facebook[15]. De esta manera, es argumentado que los precedentes sentados por esta norma representan una expansión inconstitucional de la responsabilidad penal[16], donde el gobierno podría alegar una violación al estatuto y aplicar penas desproporcionadas de manera discrecional, transformando millones de ciudadanos en criminales[17]. Además, la vaguedad de la norma resulta en provisiones redundantes que

[13] Williams, Nikki. Crime and Punishment: The Criminalization of Online Protests. Center for Digital Ethics and Policy.
[14] Wu, Tim. Fixing the worst law in technology. The new Yorker. 13/04/2013
[15] Ver, https://www.eff.org/cases/u-s-v-nosal
[16] Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78
N.Y.U. L. Rev. 1596, 1602 (2003).
[17] http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-78-5-Kerr.pdf

pueden acumularse, resultando en una suma cumulativa de las multas y penas por una misma acción[18]

Algunos de los casos a los que haré alusión demostrarán cómo la aplicación de la CFAA se ha extendido muy sobre sus propósitos originales de criminalizar el hacking, convirtiéndose en una carta en blanco para perseguir penalmente y silenciar movimientos activistas. La falta de proporcionalidad de las penas y el amplio rango de actividades inocuas que criminaliza la CFAA pone en evidencia como el criterio actual utilizado para resolver los casos más importantes sobre hacktivismo carece de un sustento racional e implica una violación de derechos fundamentales respectivos al uso de las tecnologías contemporáneas. Para observar la desproporcionalidad de las penas y la severidad con la que se ha castigado el uso tecnológico con fines activistas, hare referencia a los casos que más peso tuvieron en el debate sobre la eficacia y constitucionalidad de las normas actuales.

Aplicación de la CFAA para casos de hacktivismo

Caso de Aaron Swartz

"There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture. We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for Guerilla Open Access. With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge— we'll make it a thing of the past."

Aaron Swartz, *Guerilla Open Access Manifesto*

Uno de los casos que más impactó a la comunidad digital, despertando el debate por la necesidad de normas más claras, ha sido el del activista Aaron Swartz, co-fundador de *Reddit, Creative Commons*, y la biblioteca digital pública y gratuita *Archive.org*. En 2011 Swartz fue arrestado y acusado por utilizar la red de MIT (Massachussets Institute of

[18] Zoe Lofgren, Ron Wyden, *Introduction of Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*

Technology) para obtener acceso a la base de datos de JSTOR, descargando 4.8 millones de archivos y artículos académicos a lo largo de un periodo de 6 meses[19].

Swartz era un reconocido activista y programador que perseguía, al igual que varios miembros de la comunidad hacktivista, la idea de una internet libre e inclusiva que ponga el conocimiento a disposición de la población sin ningún tipo de barrera económica o burocrática. Debido al activismo público y vocal de Swartz, es claro que no realizo este acto con el propósito de generar ingresos a partir de los archivos obtenidos, sino bajo la idea de que los artículos científicos de JSTOR (financiados en gran parte con recursos públicos estatales) sólo pueden ser accedidos por las elites universitarias y académicas, limitando el acceso al conocimiento y a la información.

La fiscalía acusó a Swartz por 2 cargos de fraude, y 13 cargos por violaciones al CFAA, resultando en una pena cumulativa de 35 años de prisión y más de un millón de dólares en multas[20]. Frente a las presiones de la investigación, Swartz se quitó la vida, convirtiéndose en un mártir dentro de la comunidad activista digital, inspirando cientos de artículos periodísticos y legales referentes a la interpretación abusiva de esta norma para perseguir penalmente al hacktivismo.

Luego de la muerte de Swartz, el MIT realizó un reporte estableciendo que no había razón para creer que sus acciones implicaban un acceso no autorizado a la red de la universidad, y por lo tanto, la principal premisa en la que se fundaba la persecución, era falsa. Lawrence Lessig, profesor de derecho de la Universidad de Harvard[21] resumió el reporte diciendo que MIT nunca le señaló a la fiscalía que el acceso de Swartz a la red no era autorizada. El caso se fundaba en esta falta de autorización, y el estado en su ímpetu de condenar y hacer de Swartz un ejemplo para los activistas similares a él, nunca se preguntó si de hecho existía la violación que motivaba la persecución. El reporte del MIT también revelaba que la persecución de Swartz se volvió más intensa una vez que su causa se volvió pública y varias peticiones online en apoyo del activista se hicieron oír.

[19] Noam Cohen, *A Data Crusader, a Defendant and Now, a Cause*, NY TIMES (Jan. 13, 2013), http://www.nytimes.com/2013/01/14/technology/aaron-swartz-a-data-crusader-and-now-a-cause.html?_r=0.
[20] Indictment of Aaron Swartz, No. 1:11-cr-10260-NMG (Mass. Dist. Ct. July 14, 2011).
[21] Ludlow, Hacktivists on trial. Url: https://www.thenation.com/article/hacktivists-trial/

Como resultado del suicidio de Swartz, varias organizaciones como la Electronic Frontier Foundation[22] (una de las organizaciones sin fines de lucro líderes en la defensa de libertades civiles en el ámbito digital), juristas, y senadores comenzaron a plantear la necesidad de una reforma de esta norma, y presentaron la llamada "*Aaron's law*" con el fin de limitar las penas y acotar el rango de casos donde la CFAA puede ser aplicada. Dicha reforma se enfocaría en evitar la responsabilidad penal por violar los términos de servicio de un sitio y brindar un sistema de penalidades más proporcionales, manteniendo las características que hacen a la ley efectiva contra casos de hacking malicioso. A pesar de los intentos de reforma, esta no fue lograda, en gran parte por los intereses de las agencias de información que pujan por sanciones severas que desincentiven cualquier tipo de vulneración, ya sea hacktivista o no, de sus bases de datos.

Caso de Jeremy Hammond

Otro caso similar es el de Jeremmy Hammond. Siendo miembro del grupo Anonymous, fue uno de los hacktivistas partícipes en la vulneración de la base de datos de la compañía de inteligencia privada Strategic Forcasting Inc. (Stratfor). Este hack tenía el propósito de hacer pública información que demostrara el rol de la agencia en el espionaje de los ciudadanos americanos y, por sobre todo, el uso de tácticas psicológicas en contra de grupos activistas[23].

Hammond contribuyó al robo de millones de emails que eventualmente serían publicados por Wikileaks bajo el título de "*The Global Intelligence Files*", y servirían de evidencia para ilustrar cómo las empresas de seguridad privada vigilan a activistas, incluyendo a miembros de Anonymous, y el movimiento Ocuppy. Además, contribuyó a vulnerar aproximadamente 60.000 cuentas bancarias que fueron utilizadas por Anonymous para donar 70.000 USD a diversas organizaciones sin fines de lucro.

En su testimonio, Hammond declaró que su ataque se dirigió a agencias de seguridad debido a su labor para proteger los intereses gubernamentales y corporativos a

[22] Cohn, Aarons law reintroduced: CFAA didn't fix itself, url: https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself

[23]Poulsen, Anonymous hacktivist Jeremy Hammond pleads guilty for Strafor attack. Url: https://www.wired.com/2013/05/hammond-plea/

expensas de las libertades individuales, desacreditando y vilificando a activistas y periodistas que buscan una mayor transparencia. La defensa de Hammond intentó argumentar sus actos en su carácter de activista, pero al igual que Swartz, fue acusado por violar las disposiciones del CFAA y se vio forzado a declararse culpable ante la imposibilidad económica de afrontar todos los procesos judiciales de los que se lo acusaba. Se lo condenó a cumplir una sentencia de un máximo de 10 años de prisión.

Caso de Bradley Manning

Otro de los casos donde la CFAA fue aplicada es el de Bradley Manning[24]. Manning transfirió alrededor de 700.000 documentos de inteligencia clasificados al sitio Wikileaks, obtenidos durante su periodo de trabajo como un analista en inteligencia estadounidense en Irak. Entre esta información se encontraban reportes de incidentes en las guerras de Afganistán e Irak, información sobre las condiciones de detención de los prisioneros en Guantánamo Bay, y archivos de video que convirtieron al caso en un escándalo. Esta fue la mayor filtración de datos en la historia militar de Estados Unidos. Tanto Swartz, como Manning, fueron acusados de violar la cláusula del CFAA que establece que será penado todo aquel quien "*knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer…"*

Caso de Barret Brown

El último ejemplo en el cual la CFAA fue aplicada de manera abusiva, es el del periodista Barret Brown. Este periodista creo un foro público conocido como "Proyect PM", con el fin de establecer una plataforma para la discusión y publicación de información relacionada con las agencias de inteligencia privadas y como representan una amenaza contra la privacidad de la ciudadanía y los principios democráticos. Seguido de la publicación por parte de Wikileaks sobre los archivos filtrados por Hammond sobre la agencia Stratfor, Brown público en la plataforma un link a dichos archivos. A pesar de no haber participado en manera alguna en el hacking de Stratfor, actuando en su carácter de

[24]Thompson. Hacktivism: Civil disobedience or Civil Crime? Url: https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime

periodista compartiendo la información sobre el caso, el departamento de justicia estadounidense tomo sus acciones como un indicio de su participación directa con el grupo hacktivista Anonymous y Lulzec.

El departamento de justicia acuso inicialmente a Brown de 17 cargos, suficientes para obtener una pena de 105 años de prisión[25]. La defensa de Brown logro desestimar los cargos ya que incurrían en una violación constitucional de la primera enmienda, violentando la libertad de expresión manifestada a través de la publicación de un hipervínculo. Ahora bien, Brown fue declarado culpable por violar la CFAA, actuando como un agente accesorio en la distribución de información robada

La CFAA resulta útil en la persecución de casos de hacking malicioso, y si bien su redacción presenta falencias, no me parecería razonable argumentar que las victimas objeto de los actos de activismo no tengan un marco que proteja sus intereses particulares. Ahora bien, como será visto posteriormente, esta norma resulta inconsistente con los principios establecidos en el Art.19 de la DUDH y la ICCPR.

Grupos hacktivistas: Wikileaks y Anonymous

Los casos de las organizaciones hacktivistas Anonymous y Wikileaks resultan de los más interesantes para analizar, no solo por ser los grupos más prominentes y conocidos popularmente, sino por el hecho de que representan un porcentaje importante de la actividad hacktivista mundial. Las acciones de estas organizaciones han sido el catalizador fundamental que ha puesto en la agenda pública el debate sobre los medios alternativos de protesta en el ámbito digital y las dicotomías que presentan desde el punto de vista jurídico y ético.

Wikileaks es una organización internacional sin fines de lucro cuya actividad principal es la publicación y difusión de documentos confidenciales. Dichos documentos son obtenidos mediante fuentes anónimas que utilizan la plataforma virtual de Wikileaks,

[25] Ludlow, *supra What Barrett Brown's Three Remaining Charges Mean for Journalism*, Url: http://www.mintpressnews.com/barrett-browns-three-remaining-charges-meanjournalism/200479/;

diseñada para proteger la anonimidad de sus fuentes, y de esta manera evitar los riesgos, repercusiones, y la posibilidad de censura en los medios tradicionales de comunicación.

Según el sitio web de Wikileaks, el trabajo de la organización se funda en la defensa de la libertad de expresión y la libertad de prensa, en la búsqueda de una mayor transparencia por parte de tanto Estados como corporaciones privadas. Sus principios se derivan del Artículo 19 de la DUDH que establece que todos los individuos tienen un derecho a la opinar, buscar activamente y distribuir información e ideas a través de cualquier medio comunicacional independientemente de las fronteras.

Desde sus comienzos en Noviembre de 2006, Wikileaks ha publicado un estimado de 10 millones de documentos confidenciales tanto de entidades privadas como de Estados. Las publicaciones más trascendentales de la organización han girado en torno a las acciones de las fuerzas armadas estadounidenses en la guerra en Afganistán, casos de corrupción en diversas naciones, y las herramientas utilizadas por agencias estatales para el monitoreo de la población.

La publicación más reciente de Wikileaks ha sido también la más grande de su historia. El 7 de Mayo del 2017, titulada "Vault 7", la organización publicó miles de documentos donde se detallaron las actividades y capacidades tecnológicas de la United States Central Inteligence Agency (CIA) para llevar a cabo el ciberespionaje. Estos documentos explicaban de manera extensiva las herramientas y métodos utilizados por la agencia, demostrando como los criminales informáticos y las agencias estatales utilizan los mismos métodos y persiguen los mismos fines. Frente a esta filtración, el director de Tecnología y derechos humanos de Amnesty International, Elsayed Ali, publicó una interesante reflexión sobre la tendencia gubernamental actual de justificar métodos cada vez más invasivos justificándose en factores de "*seguridad nacional":*

"This new revelation again highlights the inherent difficulty of keeping information safe in the digital age. The fact that one of the world's most powerful intelligence agencies is vulnerable to losing control over its operational secrets puts into perspective the risks faced by journalists and human rights defenders in a world where governments are increasingly hostile to those who speak truth to power. o protect transparency and accountability, we must preserve the space for civil society – in today's world, this means protecting communications and data from unwarranted interference. Some of the most

shocking aspects of the leaks are indications that the CIA has known – but kept quiet – about serious security vulnerabilities in smartphones and consumer electronics used by hundreds of millions of people the world over.

It's not just the US intelligence agencies that do this – there is an unholy race among the world's security agencies to break into internet services and electronic devices, undermining information security for everyone. "A wrong reaction would be to throw our arms up in the air and give up on our privacy"[26]

Tanto *Amnesty International* como *Human Rights Watch* han expresado objeciones con las excesivas clasificaciones de seguridad y confidencialidad creadas por los gobiernos para mantener en secreto ciertos proyectos cuya existencia sin duda es de interés público. Si bien muchos de los archivos publicados por la organización han sido filtraciones (leaks), otras de sus publicaciones han sido obtenidas mediante el robo de información. Un ejemplo de ello, es el del caso de la agencia Stratfor mencionado previamente. Este caso ilustra el conflicto de intereses existente, ¿es legítima la publicación de información de interés público, aun cuando esta haya sido obtenida ilegítimamente?

Por otra parte, Anonymous es el nombre mediante el cual se distingue a una red internacional de activistas, hacktivistas y hackers que actúan en conjunto de manera descentralizada. Según Fuchs, esta es una organización *"Impredecible, anárquica, dramática, ambigua y confusa que actúa de manera colectiva y fomenta la participación libre"*. Según el manifiesto de Anonymous, el grupo se motiva en la lucha por una comunidad transparente y justa en donde la información no es censurada ni controlada por ningún agente estatal ni corporativo, en pleno respeto de los valores de la libertad de expresión y el derecho a la protesta. Además, este se caracteriza por la carencia de una organización jerárquica, la carencia de liderazgo, y la heterogeneidad de las causas que defiende.[27]

El grupo ha adoptado a lo largo de su historia diversas causas, ganando notoriedad inicialmente en 2008 gracias a su proyecto "Chanology" contra la *The Church of Scientology*. Anonymus logro hacer público un video realizado por esta organización y el

[26] Amnesty International. USA: WIKILEAKS REVELATION ON CIA HACKING UNDERSCORES HOW VULNERABLE OUR PRIVACY REALLY IS.

[27] Mikhaylova, Pag 25

actor Tom Cruise, a ser usado como herramienta propagandística para atraer nuevos adeptos. Frente a esta difusión no autorizada, y las reacciones negativas e irónicas del público, la organización inició una campaña de demandas y amenazas a cualquier sitio que publicara el video. Frente a esta respuesta, hacktivistas del grupo comenzaron a acceder a los sitios de la Iglesia, buscando demostrar como el intento de censura del video representaba una violación a la libertad de expresión, y como el culto manipulaba y extorsionaba a sus adeptos, aprovechándose financieramente de ellos, y utilizando las costosas vías legales para presionar a aquellos quienes consideran riesgosos para la organización. Anonymous ganó notoriedad exponiendo cientos de mails personales miembros del culto, organizando un ataque DDOS para dejar inoperativo sus sitios, y efectivamente convocando a miles de personas para que manifiesten de manera física frente a sedes de la iglesia alrededor del mundo.

Para el año 2010, Anonymous y su icónica imagen habían convertido al movimiento hacktivista en un fenómeno mundial. Con el ataque DDOS en contra de Visa, Mastercard, Paypal, Amazon, y PostFinance, en el marco de la llamada "*Operación Payback*", la cual fue realizada como respuesta a el bloqueo de donaciones dirigidas a Wikileaks, Anonymous demostró no solo su capacidad técnica y disruptiva, sino que contribuyó a crear la imagen mediática del hacktivismo como un movimiento de justicia vigilante. Esta idea implica el uso de violencia o amenazas por parte de agentes que no responden a autoridades estatales, y consideran que los mecanismos legales existentes van en contra del espíritu de internet.

En 2011, miembros del grupo comenzaron la llamada "OpDarkNet", con el fin de irrumpir en los servers de Freedom Hosting, utilizados por varios foros y sitios de difusión de pornografía infantil en la Dark Web. El anonimato que permite el uso de software como TOR, por un lado facilita la participación y divulgación de pornografía infantil, pero por el otro, es una herramienta utilizada por disidentes políticos y activistas que ven en estos sistemas de encriptación una manera de comunicación segura y privada. Al ser visto por la comunidad hacktivista como una herramienta protectora de la privacidad y la libertad de expresión, los ataques en contra de servidores y foros de pedofilia son acontecimientos recurrentes.

Lo mismo ha sucedido con casos de abuso animal[28], en donde la comunidad hacktivista ha hecho pública información personal de individuos filmados abusando físicamente diversos animales domésticos. Si bien este tipo de justicia vigilante resulta conflictivo, evidencia la existencia de acciones llevadas a cabo con el único propósito de brindar un bien común en los casos donde el actuar de las autoridades resulta insuficiente para la investigación de criminales de este tipo.

Estas dos organizaciones han demostrado y sometido a la mirada pública el fenómeno de las nuevas formas de protesta. Sobre todo, han puesto en foco de debate la dicotomía que se presenta cuando se demuestra la existencia de entidades gubernamentales que operan al margen de las disposiciones y garantías internacionales que protegen el derecho a la privacidad y la libertad de expresión.

El robo de información y los DDOS son en la actualidad las herramientas hacktivistas con mayor impacto y trascendencia, ya que no se valen de la prensa y sus intermediarios para hacer público un tema que debería formar parte de la esfera pública. Actuando de una manera acorde a los principios de transparencia de la información, el hacktivismo ha logrado mediante la vulneración digital, una herramienta profundamente efectiva para la realización y difusión masiva de denuncias y críticas tanto a instituciones gubernamentales, como entidades privadas y organizaciones religiosas. Es claro que muchas de las acciones de grupos de este tipo pueden ser categorizadas como delitos, pero también es cierto que en varios casos se puede observar que el hacktivismo no es una actividad inherentemente destructiva.

<u>Hacktivismo en América Latina</u>

Si bien gran parte de la actividad hacktivista, o al menos, los casos más notorios y públicamente difundidos, han tenido como objetivos a sitios y servidores operados desde Norteamérica y Europa, en los últimos 7 años, el hacktivismo ha comenzado a manifestarse en casi todas las naciones latinoamericanas. Este fenómeno se ha dado gracias a la notoriedad que ganaron los grupos activistas, y la gran influencia que han tenido en la cultura popular, demostrando la efectividad de esta vía alternativa de protesta. Además, el

[28] Max Read, "4chan on the Hunt for Puppy-Throwing Girl," *Gawker*, August 31, 2010,

fácil acceso a las herramientas necesarias para contribuir con una causa, y la creación de tecnología accesible y con un bajo costo para el usuario, han permitido que este método de protesta sea más accesible para el ciudadano promedio.

El primer caso se dio en el 2011 en Brasil, en donde miembros de un grupo afín a Anonymous, *Lulzec*, inicio ataques de denegación de servicio contra el sitio de la presidencia de la nación, el sitio de la empresa petrolera Petrobras, y la Receita Federal. Durante ese año ataques del mismo tipo se darían contra los sitios gubernamentales de Chile, Venezuela.

Tratamiento jurídico del hacktivismo en Argentina

En Argentina, en el año 2013, hacktivistas bajo el nombre de Anonymous Argentina dejaron inaccesible el sitio web del INDEC. Esto fue una reacción contra la cuestionable labor del organismo oficial de estadísticas, cuyos datos han discrepado radicalmente con la los datos provistos por consultoras privadas. El grupo hacktivista actuó denunciando los datos falsos con respecto al índice de inflación, demandando más transparencia y menos tergiversación gubernamental sobre los datos oficiales de la economía argentina.

Sebastián Bortnik, coordinador de Awarness and Research de ESET Latinoamérica, declaró que *"Sin lugar a dudas se trata de una tendencia creciente ya que cada vez es más frecuente que se realicen represalias de este tipo. Es importante, sin embargo, destacar que según la legislación de delitos informáticos en Argentina, muchas de las acciones que se están llevando a cabo son ilegales"*. El código penal argentino, al igual que la mayoría de los ordenamientos jurídicos internos de otras naciones, no contempla al hacktivismo de manera independiente, sino que se enfoca en los delitos informáticos tradicionales.

El ordenamiento argentino contiene disposiciones y objetivos similares a los planteados por la Convención de Budapest. La ley 26.388 sancionada en 2008 modifica al Código Penal Argentino incorporando los delitos informáticos y sus respectivas penas. Entre ellos, se enfatiza la distribución y tenencia de pornografía infantil (Art.2), la violación

de correos electrónicos (Art.4), el acceso ilegítimo a sistemas informáticos (Art.5), el daño informático y la distribución de malware (Art.10), y la interrupción de comunicaciones (Art.9). Si bien la norma punitiva sanciona los mismos comportamientos que la CFAA estadounidense, el ordenamiento argentino aplica penas privativas de la libertad mucho más leves, y por lo tanto permitiría aplicar parámetros más proporcionales para los casos de hacktivismo.

Tercer Capítulo: Legitimación del Hacktivismo como forma de protesta y derecho de expresión

Vistos los riesgos que genera el hacktivismo y como este fenómeno es criminalizado tanto por el derecho internacional como por la mayoría de los ordenamientos internos de los estados occidentales, es hora de analizar algunos de los argumentos utilizados por quienes creen que no solo las sanciones del derecho penal son desproporcionadas, sino que además representan una violación a garantías constitucionales protectoras del derecho a la expresión y a la protesta.

Consistencia entre el hacktivismo, el Artículo 19 de la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos

Al analizar la legitimidad del hacktivismo como fenómeno global, se ha puesto foco en la consonancia entre los ordenamientos legales internos y las garantías establecidas en los instrumentos internacionales protectores de la libertad de expresión y el derecho a la protesta. Si bien la declaración no es vinculante, su interpretación resulta útil para ponderar la contraposición de derechos en juego. El Art.19 establece lo siguiente:

"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."[29]

[29] Declaración Universal de los Derechos Humanos. Url: http://dudh.es/19/

Por su parte, el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR) se refiere a la libertad de expresión en el párrafo segundo de su Artículo 19, estableciendo lo siguiente:

"Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas."

Partiendo de esta norma, resulta necesario determinar si las restricciones establecidas en el Art.19 ICCPR se extienden a los casos de hacktivismo. En 2011, el comité de Derechos Humanos de las Naciones Unidas redactó en su comentario Nro. 34 como interpretar la disposición referente a las libertades de opinión y expresión contempladas en el Art.19 del ICCPR:

"Los Estados partes deben procurar con el mayor cuidado que las leyes sobre traición y las disposiciones similares que se refieren a la seguridad nacional, tanto si se califican de leyes sobre secretos de Estado o sobre sedición, o de otra manera, estén redactadas y se apliquen de conformidad con las condiciones estrictas del párrafo 3. No es compatible con el párrafo 3, por ejemplo, hacer valer esas leyes para suprimir información de interés público legítimo que no perjudica a la seguridad nacional, o impedir al público el acceso a esta información, o para procesar a periodistas, investigadores, ecologistas, defensores de los derechos humanos u otros por haber difundido esa información. Tampoco procede, en general, incluir en el ámbito de estas leyes categorías de información tales como las que se refieren al sector comercial, la banca y el progreso científico"

A pesar de que no se haga referencia directa a los casos de hacktivismo, esta nota resulta relevante debido al hecho que se enfatiza la protección sobre periodistas, investigadores, ecologistas, y defensores de los derechos humanos, categorías dentro de las cuales varias actividades hacktivistas podrían ubicarse. Según la comisión, las restricciones no deben ser entendidas de manera excesivamente amplia. En su Observación general Nº 27, el Comité señaló:

"las medidas restrictivas deben ajustarse al principio de proporcionalidad; deben ser adecuadas para desempeñar su función protectora; deben ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado, y deben guardar proporción con el interés que debe protegerse... El principio de proporcionalidad debe respetarse no solo en la ley que defina las restricciones sino también por las autoridades administrativas y judiciales que la apliquen"[30]*. El principio de proporcionalidad también debe tener en cuenta la forma de expresión de que se trate así como los medios por los que se difunda"*

Si bien la interpretación de estas normas dependerá de cada jurisdicción en particular, es evidente que sus disposiciones brindan un marco general que incluiría dentro de sus garantías los derechos de ciertos hacktivistas. La norma reconoce la importancia del libre intercambio de ideas a través de medios no convencionales de difusión, contemplando al mismo tiempo la necesidad de normas restrictivas que aseguren los derechos de terceros y la protección de la seguridad nacional. Según Monarch[31], una interpretación equilibrada de esta norma permitiría la condena del hacktivismo en ciertos casos, siempre y cuando se apliquen normas proporcionales que juzguen al hacktivismo de la misma manera que se juzgan casos tradicionales de protesta y desobediencia civil. Por lo tanto, penas excesivamente graves como las impuestas por la CFAA estadounidense serían inconsistentes con el espíritu de la ICCPR, ya que interpreta el uso de la tecnología como un factor agravante en los casos de activismo.

[30]ONU, Observación general Nº 27, párr. 14.
[31] Monarch. The Good Hacker: A Look at the Role of Hacktivism in Democracy.Pg.20-21

Hacktivismo como una forma de expresión legítima

Como podemos observar, el hecho de que un acto hacktivista busque transmitir un mensaje ideológico parecería no resultar suficiente como para argumentar su legitimidad como una forma de expresión. De la misma manera que el derecho a manifestarse en la vía pública no es absoluto y los actos de violencia y daños causados por ellas no deberían ser considerados como una parte del derecho a expresarse, el hacktivismo debería tratarse bajo los mismos parámetros.

Autores como Hampton plantean que los tipos de hacktivismo que impliquen el uso de herramientas como el robo de información o la manipulación de la propiedad privada, como por ejemplo los ataques DDOS realizados mediante el uso de botnets involuntarios, difícilmente puedan ser considerados una forma de expresión legítima.[32] A pesar de que el acto sea realizado con el propósito de difundir un mensaje, los medios utilizados vuelven imposible su legitimación jurídica, y para estos casos resultaría lógico encuadrar la acción como un delito informático. Por otro lado, las sentadas virtuales y los ataques DDOS y DOS llevados a cabo voluntariamente y que no causen daños permanentes, a pesar de generar inconvenientes y posiblemente algunas repercusiones económicas, parecerían deber contar con cierto grado de protección, dado sus similitudes con métodos tradicionales de protesta, o a lo sumo ser juzgados teniendo en cuenta la diferencia entre este método y aquellos más disruptivos.

Hacktivismo como forma de desobediencia civil

Uno de los argumentos más utilizados en el debate por la legitimación del hacktivismo es aquel que percibe a este fenómeno como una forma digital de desobediencia civil que contribuye al fortalecimiento del sistema democrático[33]. Este concepto implica la comisión de un acto que no recurra a la violencia, pero que viole conscientemente la letra de la ley con el fin de expresar una protesta en contra de dicha norma o el sistema legal del cual emana, realizando un llamado de atención hacia las injusticias creadas por ella.

[32] Hampson, p.24

[33] Himma, p.2

Esta línea de pensamiento considera que los actos encuadrables bajo la idea de desobediencia civil no solo están moralmente justificados, sino que representan una conducta positiva que contribuye a la redacción de normas más justas[34]. Por lo tanto, no implica desobedecer la ley de manera clandestina, sino hacerlo de manera pública y de modo que hacerlo no genere daños a terceros. Si bien hemos visto múltiples casos donde el hacktivismo no es totalmente consistente con los principios de la desobediencia civil, este concepto permite distinguirlo del ciberterrorismo (método que utiliza medios violentos) y los delitos cibernéticos (que están motivados por el beneficio personal).

Himma, en su análisis del hacktivismo como forma desobediencia civil, plantea ciertos parámetros que ayudarían a determinar el grado de legitimidad de determinado comportamiento enmarcado bajo esta idea. Entre ellos se encontraría el cálculo del daño generado por un determinado acto, que dependerá en gran parte del tipo de organización a la que un determinado ataque se dirija. El hacktivismo puede tener como objetivo sitios web privados, públicos, que pueden llevar a cabo actividades comerciales o no. Es posible inferir que un ataque al sitio de una organización privada con fines comerciales pueda generar daños patrimoniales más elevados a un número mayor de individuos, en comparación de aquel en contra de un sitio público y con fines meramente informativos. Ataques DDOS dirigidos a individuos privados (como por ejemplo, el bloqueo de un blog o un foro de discusión) podrían tener leves efectos económicos, pero se estaría vulnerando la libertad de ese individuo a expresarse libremente y compartir sus ideas.

El otro parámetro que utiliza Himma para analizar el hacktivismo, es el respectivo al método utilizado. Al igual que la mayoría de la literatura académica sobre el tema, plantea el hecho de que métodos como el graffitti y las sentadas virtuales generan daños y disrupciones comparativamente mucho menores que los ataques DDOS. Ahora bien, estos parámetros no son absolutos y aplicables a todos los casos, de modo que la protección del hacktivismo debería ser considerada teniendo en cuenta las circunstancias de cada caso en particular.

Según la visión de Hannah Arendt respecto de la legitimidad de los actos de desobediencia civil, el sistema democrático debería dejar un margen legal que permita el

[34] Id, p.2

conflicto y la pluralidad de ideas. Si bien el concepto de legitimar un acto que va en contra de la ley resulta paradójico, la institucionalización de la desobediencia civil actúa como un factor que equilibra las falencias legislativas y los aspectos negativos no previstos en la redacción de normas. De esta manera, dichos actos no deberían ser observados como una violación que atenta contra el orden social, sino que deberían ser vistas como un síntoma de las fallas e injusticias creadas por ciertas leyes.

Otro argumento que sigue esta línea es el que presenta Samuel, que se basa en la idea de "*Policy circunvention*". Similar al concepto de desobediencia civil, esta es una respuesta estratégica y política frente a una ley, una regulación o una decisión judicial, donde se protesta su aplicación injusta o impráctica. Esta estrategia busca combatir los efectos de una norma considerada ilegítima, creando beneficios que no sean exclusivos a los partícipes, diferenciándose de una típica acción criminal. Además, tiene efectos como crear concientización sobre un tema, y contribuir al cambio normativo. Un ejemplo de ello, es el caso de la organización activista *Hacktivismo*, un proyecto diseñado para evadir las normas que censuran el acceso a internet en China y otros regímenes no democráticos como Arabia Saudita, y Túnez, en donde el acceso a internet se encuentra limitado por el estado. Mediante el desarrollo de software de acceso libre para evadir los Firewalls de estas naciones, *Hacktivismo* logra crear beneficios concretos no solo en materia de libertad de expresión, sino que también generando consciencia sobre los riesgos de la censura de internet y su poder para esquivar barreras al acceso a la información de manera injustificada.

La aplicación de este concepto ha sido extensamente debatida debido a la conflictividad inherente en considerar una violación de la ley parte de la libertad a expresarse. No se trata de un discurso, sino de una acción que toma como premisa la existencia de casos en donde la violación de la ley es moralmente aceptable, e incluso obligatoria cuando se trata de una ley manifiestamente injusta e inmoral. Esta corriente de pensamiento considera al hacktivismo como una actividad cuya legitimad es moralmente justificada debido a su carácter de activismo político, ya que en la mayoría de los casos, los ataques a sitios gubernamentales y corporativos demuestran estar motivados por razones válidas que brindan un beneficio social. Pero al igual que Hampton, la conclusión a la que

arriban es similar: A pesar de que el hacktivismo se asimile a actos de desobediencia civil, y por lo tanto pueda ser considerada una forma legítima de participación política, debido a la naturaleza de las herramientas utilizadas, los casos deben ser analizados de manera particular teniendo en consideración el grado de daños e inconvenientes creados por el medio utilizado.

Siguiendo esta misma línea, Widney Brown, directora del departamento de derecho internacional de Amnesty International, ha considerado que el uso de métodos no convencionales de activismo en defensa de los principios de libertad de expresión y protesta se encuentra justificados siempre y cuando estos no violen los derechos de privacidad y seguridad de terceros.[35]

De esta manera, aquellos que defienden al hacktivismo como una actividad legitima de participación política, y una manifestación de protesta necesaria dentro de un sistema democrático, lo plantean como una extensión de derechos fundamentales existentes como lo es el derecho a la protesta en la vía pública, y la libertad a expresarse libremente sin temor a la censura.

En la antigüedad las manifestaciones de descontento y preocupación se llevaban a cabo en las plazas y calles públicas, ya que eran los sitios que maximizaban el alcance de un mensaje. Hoy en día, la idea del hacktivismo como manifestación política resulta lógica frente al nuevo posicionamiento de internet como el centro donde todos los debates confluyen a escala global. El medio resulta idóneo para transmitir ideas y realizar reclamos alcanzando a un número mayor de individuos, y por lo tanto aumentando las chances de brindar atención a un tema determinado.

El conflicto de la libertad de expresión

Con respecto a la libertad de expresión, Cohen señala la importancia de garantizar su protección para el fortalecimiento democrático de un estado. La democracia se funda en el principio de soberanía popular, que requiere el libre discurso entre los ciudadanos. Crear barreras a dicho discurso crea una inequidad política donde los temas discutidos en la

[35]Ryan, Anonymous and the Arab uprisings, url: http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

agenda pública son restringidos, limitando el acceso a la información, y por lo tanto reduciendo la calidad del discurso.

Ahora bien, muchas de las manifestaciones hacktivistas implican la alteración o bloqueo del discurso de otros individuo u organización, remplazando un mensaje por otro, y por lo tanto, silenciando temporalmente un discurso. Este, lógicamente, es un punto que genera resistencia en la consideración del hacktivismo como un medio de expresión legítimo, pero debe ser considerado el hecho de que no todos los hacktivistas se manifiestan de manera que su libertad de expresión implique la supresión del derecho de un tercero. Existen aquellas organizaciones como "*Hacktivismo*", que están en contra del uso de herramientas informáticas como el graffitti virtual y las sentadas virtuales, que busquen interferir con los derechos de un tercero, sosteniendo una visión absoluta del derecho a expresarse. Por otro lado, están aquellos quienes si bien creen en el respeto de la libertad de terceros, sostienen la necesidad de que en ciertos casos, dichos actos son necesarios y justificados, dada las inequidades en la capacidad de ser oído en una plataforma tan vasta como lo es internet. Debido al exceso de información y la limitada audiencia, lograr llamar suficiente atención a un terma en particular se vuelve una tarea dificultosa, y el hacktivismo opera de modo de equilibrar la capacidad de ser oído.

En Estados Unidos, el conflicto principal respecto de la libertad de expresión ha sido el alcance protector de la primera enmienda de la constitución. La cuestión a dilucidar ha sido como interpretar la norma frente a la idea de que la constitución solo protege las manifestaciones de protesta en el contexto de la esfera pública, y solo brinda protección contra el actuar gubernamental. La dificultad se presenta al intentar resolver si los sitios administrados por entes privados o por agencias estatales forman parte de la esfera pública, o si las interferencias a ellos implican una vulneración efectiva al derecho a la propiedad.

El hecho de que un ciber ataque reemplace un discurso por otro, inevitablemente hace que el hacktivismo sea inconsistente con las nociones de la libertad de expresión en la primera enmienda. Ahora bien, dado que gran parte de las plataformas virtuales son administradas de manera privada, especialmente aquellas con más notoriedad y alcance público, ¿Sería prudente expandir la definición de "esfera pública" para incluir sitios privados dentro de su definición? Para responder esta pregunta, debería realizarse un

análisis minucioso y un balance entre los conflictos de intereses, tarea extremadamente compleja, por lo que su justificación difícilmente sea aceptada jurídicamente.

Frente a este problema, Zatz propone una idea creativa que se funda en la creación de espacios públicos digitales a través de la implementación de Pop-Ups adyacentes al sitio que sería atacado. Este método lograría efectivamente transmitir el mensaje deseado a un público específico, evitando el entorpecimiento del sitio atacado, y el carácter censurador del acto. No se reemplaza un discurso por otro, sino que se agrega un mensaje adyacente que puede ser ignorado por los usuarios del sitio.

Otro punto discutido es el referente al lugar que tiene la anonimidad en el discurso democrático. Por un lado, es criticado el hecho de que el hacktivismo se vale de esta característica para evitar su persecución y las consecuencias legales de sus acciones, por lo que le permite a cualquier individuo realizar un discurso o un acto sin tener que lidiar con las responsabilidades que ello implica. De esta manera, la anonimidad es algo que separa al hacktivismo de las formas tradicionales de protesta, siendo una característica destructiva que va en contra de del dialogo abierto democrático.

Por otro lado, la anonimidad es vista como un factor esencial para el libre discurso, al separar al mensajero del mensaje, y permitirles a los individuos manifestar ideas controversiales que de otra manera no podrían hacer públicas, debido a las consecuencias sociales de hacerlo. Nuevamente, tanto los efectos positivos como negativos de la anonimidad pueden manifestarse en la realidad, dependiendo del tipo de acción del que se trate. Actos de hacktivismo bajo el concepto de "*Political Cracking*", es decir, realizados en rechazo a cualquier tipo de norma, tienden a ser realizados de manera de no dejar rastros ni evidencia que permita identificar a los partícipes con el fin de evadir repercusiones legales. Actos de hacktivismo más expresivos sueles ser realizados bajo pseudónimos que le permiten al actor dejar una marca personal que permita identificar sus acciones. La anonimidad no opera de forma absoluta para evadir la ley, sino que es utilizada de diferentes maneras como herramienta política y estratégica para transmitir mensajes.

La puja por una reforma jurídica sobre el activismo digital

En 2013 Anonymus realizó una petición al gobierno estadounidense para reconocer a los DDOS como una forma valida y legítima de protesta protegida por la primera enmienda de la constitución. La organización planteó una analogía entre los DDOS y el caso de las manifestaciones parte del movimiento "Occupy", en donde la protesta implicaba la ocupación de un espacio físico para crear una disrupción y lograr llamar la atención mediática y popular a modo de hacer oír su mensaje. Los DOS y DDOS, según la postura de Anonymous, serían su contraparte digital, a diferencia que las herramientas digitales hacktivistas resultan exponencialmente más eficientes en cuestión a los recursos necesarios para ser llevados a cabo y el número de personas requeridas para transmitir un mensaje político.

Esta postura es debatida y apoyada por varios juristas y activistas, que ven la necesidad de una reforma legislativa que contemple el uso del DDOS como una herramienta con fines políticos y sociales, y no criminalice severamente un comportamiento cuya legitimidad e impacto depende enteramente de su uso y contexto. Esta es la idea sostenida por Jay Leiderman, un abogado que ha representado a varios hacktivistas notorios, y uno de los juristas más vocales con respecto a la necesidad de una reforma. Según Leiderman, la normativa vigente no contempla la variante del hacktivismo como una herramienta a favor de los derechos civiles, la transparencia, la libertad de expresión, y el derecho a la protesta.

El primer caso internacional en donde se reconocieron los argumentos legales y éticos hacktivistas fue el caso del ciudadano alemán Andreas-Thomas Vogel, administrador del sitio web *Libertad.de* durante la acción colectiva en contra de Lufthansa Airlines en 2001. Se lo arresto por fomentar el ataque DDOS en el sitio, y causar daños económicos a la aerolínea, por lo cual se lo sentenció a una multa o 90 días de prisión. La corte superior estableció que sus demostración online no constituía un uso de la fuerza ni un método de coerción contra la aerolínea, sino que era una manera de influenciar la opinión pública[36]

[36] "Higher Regional Court says online demonstration is not force," *Heise Online*, 2006.

Ahora bien, en el futuro difícilmente los DDOS sean parte del repertorio de protestas aceptada popular y legalmente en los países occidentales. Son recursos de fácil acceso que permiten bloquear el acceso a cualquier sitio, desde blogs donde periodistas y activistas comparten sus ideas, a sitios oficiales de organizaciones de derechos humanos. Los DDOS resultan una herramienta muy efectiva para silenciar puntos de vista. Ahora bien, los individuos que demandan una nueva interpretación legal de estos métodos no niegan esta faceta destructiva de los DDOS como una forma de ataque, pero afirman que el hecho de que los estados no contemplen su contracara como una forma de protesta implica un mal mayor.

Dentro de las organizaciones activistas que han trabajado por la legitimación del hacktivismo, se encuentra la organización Británica de derechos humanos "Article 19". Esta ha reconocido la necesidad de una actualización del marco jurídico, y frente a ella ha planteado una serie de principios con el objetivo de promover nuevas normas que contemplen las nuevas tecnologías y formas de protesta. Estos principios buscan alcanzar una definición más clara respecto de los medios de protesta legítimos, incorporando las vías digitales, el concepto de desobediencia civil, las obligaciones estatales referentes al respeto de instrumentos normativos internacionales, y el rango limitado de restricciones a estos derechos.

Según la organización, Wikileaks y la comunidad hacktivista representan una extensión de los medios de comunicación tradicionales, y actúan como un canal que permite la publicación de información relevante sobre corrupción, fraude y prácticas corporativas ilegales que de otro modo difícilmente se harían públicas.

La organización *The Electronic Frontier Foundation* es otro ejemplo de la unión de abogados, especialistas informáticos, periodistas y activistas que reconocen la importancia de defender las libertades civiles en el ámbito digital. Desde su fundación en 1990, la organización ha denunciado el gobierno federal estadounidense, La Comisión Federal de Comunicaciones, y diversas corporaciones electrónicas respecto a temas como limitaciones al desarrollo tecnológico independiente (Bernstein v. US Department of Justice), la libertad de expresión en el ámbito digital (Steve Jackson Games v. Secret Service Case Archive), la

invasión injustificada de la privacidad por parte de agencias estatales (USA v. Pen Register), y el fair use (Huntsman v. Soderbergh).

Conclusiones

El crecimiento del hacktivismo como medio de protesta ha sido el resultado de dos factores principales. En primer lugar, el creciente rol de la tecnología en todas las facetas de la vida moderna, que ha expandido las vías de comunicación, y democratizado el acceso a la información. Internet ha provisto nuevos canales eficientes de participación política que han facilitado el discurso democrático, permitiendo una comunicación instantánea y accesible. El segundo factor es el referente al contexto global de crisis económica, política e institucional en el que se desarrolla el hacktivismo, que ha contribuido a la evolución del hacking y a un mayor compromiso político. Los aspectos negativos de la globalización, en conjunto con el creciente poderío estatal y corporativo crearon un contexto en donde las posturas disidentes inevitablemente convergerían hacia el uso tecnológico para expresarse y manifestarse.

La información publicada por grupos hacktivistas como Wikileaks y Anonymous, en conjunto con informantes como Edward Snowden, han demostrado el crecimiento del poderío corporativo y estatal, que en pos de garantizar la seguridad nacional, se valen de herramientas cada vez más invasivas, utilizando la tecnología para incurrir en procedimientos que vulneran principios democráticos fundamentales.

Los intentos gubernamentales por controlar internet solo han despertado mayor desconfianza en las autoridades y en los propósitos e intereses que persiguen las normas, convirtiendo al hacktivismo en una consecuencia frente a la corrupción y la falta de transparencia corporativa y gubernamental. El tratamiento del hacktivismo como una amenaza de seguridad nacional legitima la sanción de normas cada vez más severas e ignora las implicancias sobre libertad, seguridad y privacidad.

El hacking sin duda representa una amenaza a la privacidad y la protección de la propiedad privada, pero la solución legislativa de redactar normas penales severas no logra

prevenir los riesgos, y en caso de hacerlo, lo hace a expensas de la libertad de expresión y el derecho a la protesta.

Con la creciente digitalización de la información, y el creciente deseo por hacer pública la información considerada de interés público por parte de activistas que adoptan las nuevas tecnologías con el fin de cumplir sus objetivos de protesta y expresión, resulta evidente la necesidad de un ordenamiento jurídico claro que por un lado proteja la privacidad y la propiedad privada, y por el otro, esté en consonancia con los principios ilustrados en el ICCPR y la DUDH. En la actualidad, la aplicación de normas creadas con el fin lidiar con las amenazas presentadas por el hacking resultan desproporcionadas al no contemplar la distinción entre el uso de estas herramientas con fines personales y su uso como método de protesta y expresión. Al no existir dichas normas, la defensa jurídica de este tipo de activismo carece de posibilidad de fundamentar sus actos basándose en tratados internacionales y principios democráticos.

Las innovaciones tecnológicas que facilitan y reducen los costos de contribuir al debate público deberían ser fomentadas en un sistema con valores democráticos. Esto sin olvidar la faceta de la tecnología que facilita el acceso a actividades destructivas. En el caso del hacktivismo, la misma tecnología que por un lado es útil en la organización y movilización de individuos separados geográficamente pero con ideales comunes, también permite separar el mensaje del mensajero, reduciendo los costos de actuar destructivamente gracias al anonimato inherente en internet. El desafió para la ley se convierte en el fomento de la aplicación tecnológica para fortalecer el debate público y la participación ciudadana, manteniendo a raya la aplicación destructiva de esa misma tecnología.

El hacktivismo le permite a un ciudadano promedio la habilidad de manifestar sus ideas y descontentos contra organizaciones privadas y estatales de una manera accesible, e independiente de barreras geográficas. La aplicación de leyes sobre delitos informáticos no desincentivara la existencia y el desarrollo de nuevos métodos hacktivistas, sino que por el contrario, la falta de interés estatal y legislativo en fomentar formas de protesta y expresión en el ámbito digital, criminalizando de manera uniforme todas las actividades que involucren las mismas herramientas informáticas, producirá una división y oposición más profunda. La re conceptualización de un marco legal actualizado resulta la única manera de

salvaguardar los aspectos positivos de este tipo de activismo, mitigando al mismo tiempo su faceta negativa.

Es claro el hecho de que la tecnología avanza a una velocidad que supera ampliamente la capacidad de las instituciones y los ordenamientos jurídicos en adaptarse a ellas. La adopción de instrumentos internacionales es un proceso extremadamente lento, pero en la nueva era digital en la que vivimos, la capacidad de la ley en actualizarse en conjunto con los avances tecnológicos será una absoluta necesidad, ya que tanto las instituciones como la tecnología están condenadas a evolucionar, o de lo contrario, caer en la obsolescencia.

Bibliografía

Allnut, Luke. Hacktivist's Advocate: Meet the Lawyer Who Defends Anonymous. The Atlantic. 3/10/2012. URL: https://www.theatlantic.com/international/archive/2012/10/hacktivists-advocate-meet-the-lawyer-who-defends-anonymous/263202/

Arendt, H. (2012). *In der Gegenwart: Übungen im politischen Denken II*. München: Piper. In English: Arendt, H. (1972). *Crises of the republic: Lying in politics, civil disobedience on violence, thoughts on politics, and revolution* (Vol. 219). Houghton Mifflin Harcourt.

Argentina. Ley 26.388 del Codigo Penal, sancionada el 24 de Junio del 2008. Url: http://www.oas.org/juridico/PDFs/arg_ley26388.pdf

Article 19. org Url: https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf

Bortnik, Sebastián. "El canon en Argentina: Anonymous y el hacktivismo." WeLiveSecurity. June 29, 2011. Accessed May 10, 2017. Url:

http://www.welivesecurity.com/la-es/2011/06/29/canon-argentina-anonymous-hacktivismo/.

Burgos Pino, Edixela Karitza. EL HACKTIVISMO: ENTRE LA PARTICIPACIÓN POLÍTICA Y LAS TÁCTICAS DE SUBVERSIÓN DIGITAL. Razon y Palabra. Url: http://www.razonypalabra.org.mx/N/N88/Varia/05_Burgos_V88.pdf

Council of Europe. Convention on Cybercrime. Budapest, 2001. Url: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Cox, Joseph. "The History of DDoS Attacks as a Tool of Protest." *Motherboard*. Primero de Octubre, 2014. https://motherboard.vice.com/en_us/article/history-of-the-ddos-attack.

Cox, Joseph. DDoS isn't Going to be a Legal Form of Protest Any Time Soon. The Daily Dot. 19/6/2014. Url: https://www.dailydot.com/layer8/ddos-attack-political-protest/

Data Breach Investigation Report. Verizon RISK Team y la Policia Federal Australiana. 2012 Url: **http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.**

Denning, Dorothy. The Rise Of Hacktivism. Georgetown Journal. 8/9/2013. Url: http://journal.georgetown.edu/the-rise-of-hacktivism/

Dergaraberian, Cesar. "Hacktivistas" comenzaron el 2013 "tomando de punto" a varios sitios web del Gobierno argentino. IProfesional. 5/2/2013. Url: http://www.iprofesional.com/notas/153915-Hacktivistas-comenzaron-el-2013-tomando-de-punto-a-varios-sitios-web-del-Gobierno-argentino

Eordogh, Fruzsina. Silicon Valley Is Stonewalling Efforts to Amend the Law Imprisoning Hacktivists . Motherboard. 16//7/2014. Url: https://motherboard.vice.com/en_us/article/silicon-valley-is-stonewalling-efforts-to-amend-the-law-imprisoning-hacktivists

Ernstt, Douglas. NSA releases privacy-violation documents on Christmas Eve. *The Washington Times - Friday, December 26, 2014. Url: http://www.washingtontimes.com/news/2014/dec/26/nsa-releases-privacy-violations-accounts-response-/*

EVhAck. 10 lecturas sobre hacktivismo. *@rroba*. URL: http://sindominio.net/~xabier/textos/evhack/10_lecturas_hacktivismo.pdf

Fish, Adam y Follis, Luca. Hacktivists aren't terrorists – but US prosecutors make little distinction. Phys. 29/7/2015. Url: https://phys.org/news/2015-07-opinion-hacktivists-terrorists-prosecutors-distinction.html

Fung, Archon. *What the Snowden Affair Tells Us About American Democracy*. Boston Review, 2013. Url:http://www.bostonreview.net/blog/what-snowden-affair-tells-us-about-american-democracy

Greene, David y Rodriguez, Katitza..NSA Mass Surveillance Programs Unnecessary and Disproportionate.Electronic Fronteer Fundation. Url: https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf

Greene, Tim. Can $1M in damages be accurate in a website defacement?. Network World. 9/10/2015. Url: http://www.networkworld.com/article/2991398/security/can-nearly-1m-in-damages-be-accurate-in-a-websit-defacement.html

Grozeva, Lily. What Is Website Defacement?.5/03/2013. Url: http://www.websitepulse.com/blog/what-is-website-defacement

Hampson, Noah. Hacktivism: A New Breed of Protest in a Networked World. *Boston College of International and Comparative Law Review*. 2012

Himma, Kenneth Einar, Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified? (September 5, 2005). Available at SSRN: https://ssrn.com/abstract=799545 or http://dx.doi.org/10.2139/ssrn.799545

Hofmann, Marcia y Reitman Rainey. Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service. Electronic Frontier Fundation. 4/2/2013. Url: https://www.eff.org/issues/cfaa

Hughes, Thomas. Hacktivism to Balaclava Punk: Protest Must Be Protected in All Its Forms. Huffington Post. 22/06/2015. Url: http://www.huffingtonpost.co.uk/thomas-hughes/right-to-protest_b_7620410.html

Jauregui, Andres. Anonymous DDoS Petition: Group Calls On White House To Recognize Distributed Denial Of Service As Protest. Huffington Post. 1/12/2013. Url: http://www.huffingtonpost.com/2013/01/12/anonymous-ddos-petition-white-house_n_2463009.html

Jordan, Tim, and Paul A. Taylor. *Hacktivism and cyberwars: rebels with a cause?* London: Routledge, 2004.

JPerry, Why DDoS Attacks are Not Free Speech. Economic Crime and Cybersecurity institute at Utica College. 29/1/2013. Url: http://www.ecii.edu/why-ddos-attacks-are-not-free-speech/

Kaplan, Dan. Hacktivist-led DDoS is now the most common type, study finds. SC Magazine. 8/2/2012. Url: https://www.scmagazine.com/hacktivist-led-ddos-is-now-the-most-common-type-study-finds/article/541613/z

Kaplan, Jeremy A. We want you, Say hacktivists…But is it legal?. *Fox News*. 9/12/2010. URL: http://www.foxnews.com/tech/2010/12/09/wikileaks-operation-payback-hacktivists-legal.html

Kates, Graham. The Future of 'Hacktivism'. The Crime Report. 21/1/2013. Url: https://thecrimereport.org/2013/01/21/2013-01-the-future-of-hacktivism/

Keizer, Gregg. 'Hackers' deface UN site. Computer World. 12/08/2007. Url: http://www.computerworld.com/article/2543082/security0/-hackers--deface-un-site.html

Kelly, Meghan. Petition asks White House to make DDoS attacks a form of protest. Venture Beat. 10/1/2013. Url: https://venturebeat.com/2013/01/10/ddos-petition/

Kerr, Orin. *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*. New york Law Review. Url: http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-78-5-Kerr.pdf

Larson, Dave. Cyber Warfare or Hacktivism? DDoS Attacks Can Be Used Either Way. Corero. 24/3/2016. Url: https://www.corero.com/blog/710-cyber-warfare-or-hacktivism-ddos-attacks-can-be-used-either-way.html

Leetaru, Kalev. Alphabet's Project Shield And Eliminating DDOS Attacks On Free Speech. Forbes. 9/2/2017. Url: https://www.forbes.com/sites/kalevleetaru/2017/02/09/alphabets-project-shield-and-eliminating-ddos-attacks-on-free-speech/#297015996dbf

Leiderman, Jay. Why DDOS is Free Speech. Leak Source. 23/1/2013. Url: https://leaksource.wordpress.com/2013/01/23/why-ddos-is-free-speech/

Liederman, Jay. Justice for the Paypal Wikileaks Protesters: Why DDOS is Free Speech. The Guardian. 22/1/2013. Url: https://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech

Li, Xiang. 2013. Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime. *Harvard Journal of Law & Technology*. Volume 27, Number 1 Fall 2013

Lonergan, Kevin. The rise of hacktivism: where does the law stand and can we protect ourselves? *Information Age*. 7/4/2016. Url: http://www.information-age.com/rise-hacktivism-where-does-law-stand-and-can-we-protect-ourselves-123461215/

Lovink, Geert y Riemens, Patrice. Twelve theses on Wikileaks. *Le monde diplomatiqe*.2010. Url: http://mondediplo.com/openpage/twelve-theses-on-wikileaks

Ludlow, Peter. Hacktivists on Trial. *The Nation*. 4/12/2013. Url: https://www.thenation.com/article/hacktivists-trial/

Manion, Mark y Goodrun, Abby. Terrorism or Civil Disobidence. *Drexel University*. Url: http://www.csis.pace.edu/cis101/CIS_101_Fall_2007_Spring_2008/LearningPodTopics/SocialResponsibility/Terrorism-or-Civil-Disobedience.pdf

Mattern, Benjamin. Cyber Security in Latin America: Past and Future. Council on Hemispheric Affairs. URL: http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/

McLaughlin, Victoria. Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind?. Program in Political and Social Thought at the University of Virginia. 2012

McVeigh, Karen. Hacktivist anger over US government´s "ludicrous" Cyber Crackdown. 24/1/2013. Url: https://www.theguardian.com/technology/2013/jan/24/hacking-us-government-cyber-crackdown

Mikhaylova, Galina. *THE "ANONYMOUS" MOVEMENT: HACKTIVISM AS AN EMERGING FORM OF POLITICAL PARTICIPATION*. Tésis de grado, Texas State University, 2014. Url: https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1

Monarch, Benjamin. The Good Hacker: A Look at the Role of Hacktivism in Democracy (May 8, 2015). Available at SSRN: https://ssrn.com/abstract=2649136 or http://dx.doi.org/10.2139/ssrn.2649136

Morozov, Evgeny. Denial-of-service attacks are just another form of civil disobedience. Slate. 13/12/2010. Url: http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html

Paganini, Pierluigi. They are Not What You Think They are … They are Hacktivists. Security Affairs. 6/4/2012. Url: http://securityaffairs.co/wordpress/4986/cyber-crime/they-are-not-what-you-think-they-are-they-are-hacktivists.html

Paget, François. Hacktivismo: El ciberespacio como nuevo medio de difusión de ideal políticas. Mc Afee. Url: https://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf

Pangburn, DJ. The 'Hacker Wars' Documentary Does Hacktivism No Favors. *VICE*. 22/10/2014. URL: https://www.vice.com/en_us/article/the-hacker-wars-documentary-does-hacktivism-no-favors-1023

Pascucci, Matthew. Can we stop hacktivism?. SC Magazine. 4/10/2011. Url: https://www.scmagazine.com/can-we-stop-hacktivism/article/547750/

Poulsen, Kevin. "Anonymous Hacktivist Jeremy Hammond Sentenced to 10 Years in Prison" Wired. 15/11/13. Url: https://www.wired.com/2013/11/hammond-sentence/

Protesta Social Y Derechos Humanos. Instituto Nacional de Derechos Humanos. Url: http://acnudh.org/wp-content/uploads/2015/04/PROTESTA-SOCIAL.pdf

Richards, Neil M. The Dangers of surveillance. *Harvard Law Review*. Url: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf

Roberts, Paul. Verizon: Hacktivists steal most data in 2011. Threat Post. 22/3/2012. Url: https://threatpost.com/verizon-hacktivists-steal-most-data-2011-032112/76350/

Samuel, Whitney Alexandra. *Hacktivism and the future of political participation*. Tésis doctoral, Harvard University, 2004. Url : http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

Sasso, Brenan. NSA Spying Violates Privacy Rights, EUCourt Rules. National Journal, 2015.Url: http://www.defenseone.com/news/2015/10/nsa-spying-violates-privacy-rights-eu-court-rules/122580/

Schneier, Bruce. Schneier on Security. 13/6/2013. Url: https://www.schneier.com/blog/archives/2013/06/essays_related.html

Shahani, Aarti. US puts Internet protests on trial as part of PayPal 14 prosecution. Aljazeera. 29/10/2013. Url: http://america.aljazeera.com/articles/2013/10/29/prosecutors-put-paypal14andinternetprotestontrial.html

Smith, MS. EFF on cyber-attack against hacktivists: CFAA for you; impunity for feds. Network World. 5/2/2014. Url: http://www.networkworld.com/article/2226300/microsoft-subnet/eff-on-cyber-attack-against-hacktivists--cfaa-for-you--impunity-for-feds.html

Stuart, Sophia. DDoS Attacks: Legitimate Form of Protest or Criminal Act? PC Magazine. 20/10/2014. Url: http://www.pcmag.com/article2/0,2817,2469400,00.asp

Slobogin, Christopher. *Privacy at Risk*. Chicago: The University of Chicago Press, 2007. *Google Books*. Web. 08 Nov. 2013.

The Right to Protest. Principles on the protection of human rights in protests. Article 19. 2016.
Url:https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf

Thompson, Christine. Hacktivism, Civil Disobidience or Cyber Crime?. Pro Publica. 18/1/2013. URL: https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime

Torres Soriano, Manuel R. Siete Lecciones no aprendidas de Anonymous. Instituto Español de Estudios Estrategicos. 2013.

Url:http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO122-2013_Anonymus_Manuel_R.TorresSoriano.pdf

Vamosi, Robert. How Hacktivism Affects Us All. PC World. 6/09/2011. Url: http://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html

Veal, Vangie. DDoS attack - Distributed Denial of Service. Webopedia. Url: http://www.webopedia.com/TERM/D/DDoS_attack.html

Vijayan, Jaikumar . 'Anonymous' arrests tied to PayPal DDoS attacks, FBI says. Computer World. 19/8/2011. Url: http://www.computerworld.com/article/2509264/cybercrime-hacking/-anonymous--arrests-tied-to-paypal-ddos-attacks--fbi-says.html

Waqas, Amir. "Anonymous DDOS Brazilian Government Websites Because Rio Olympics". *Hackread*. URL: https://www.hackread.com/anonymous-ddos-brazilian-government-websites/

Williams, Nikki. Crime and Punishment: The Criminalization of Online Protests. Center for Digital Ethics and Policy. 10/9/2015. Url: http://digitalethics.org/essays/the-criminalization-of-online-protests/

Wikileaks. Visitado por última vez el 4/5/2017. Url: https://wikileaks.org

Wu, Tim. Fixing the worst law in technology. The new Yorker. 13/04/2013. Url: http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

Yoon, Joyce M. *Edward Snowden, Criminal or Patriot: Media Coverage of National Security Agency Document Leaks.* Digital Commons @ Andrews University, 2015. Url: http://digitalcommons.andrews.edu/cgi/viewcontent.cgi?article=1115&context=honors

Zatz, Noah D, *Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment*, 12 HARV. J.L. & TECH. 149, 152.