UnilaSalle Editora

REDES – REVISTA ELETRÔNICA DIREITO E SOCIEDADE
http://revistas.unilasalle.edu.br/index.php/redes
Canoas, vol.4, n. 2, novembro 2016
http://dx.doi.org/10.18316/2318-8081.16.28

Hacktivismo e ativismo digital na sociedade da informação

Irineu Francisco Barreto Junior[1]

Henrique Auler[2]

Marco Antonio Barbosa[3]

Artigo submetido em: 25/07/2016

Aprovado para publicação em: 29/08/2016

Resumo: Este artigo tem o objetivo de analisar o conceito de*hacktivismo*, suas diferenças em relação ao ativismo digital e aos crimes cometidos nos meios digitais. Busca-se ainda analisar sua possível aproximação com as práticas de desobediência civil. Foram utilizados textos acadêmicos, bem como relatos de participantes do *hacktivismo* e do ativismo digital, para delinear a área de atuação de cada movimento. Este texto discute como o ativismo *hacker* e o digital, apesar de semelhantes, possuem diferenças essenciais, tornando-os movimentos distintos. Também foi analisada a abordagem da mídia tradicional ao tratar manifestações políticas legítimas como crimes, apesar das semelhanças apenas ocorrerem nas técnicas empregadas. Através dessa distinção, poderão os operadores do direito de forma mais precisa classificar a espécie de ação exercida, evitando assim abusos e injustiças contra os ativistas.

Palavra-chave: Ativismo Digital; Hacktivismo; Internet; Sociedade da Informação.

Hacktivism and digital activism inside the information society

Abstract: This article aims to analyze the conception of hacktivism, its differences in relation to digital activism and crimes committed in digital media. It also seeks to analyze possible appoach with the practices of civil disobedience. Academic texts were used as well as reports of participants in hacktivism and digital activism to delineate the area of action of each movement. This article discusses how hacker and digital activism, although similar, have essential diferences, making them different movements. We also analyzed the traditional media approach in dealing with legitimate political manifestations as crimes, although similarities only occur in the techniques used. Through this distinction,

[1] Doutor em Ciências Sociais pela PUC-SP; Docente do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). E-mail: neubarreto@hotmail.com

[2] Advogado e bacharel em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). E-mail: henriqueauler@hotmail.com

[3] Doutor em Direito pela Universidade de São Paulo; Docente do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). E-mail: marco.barbosa@fmu.br

lawmakers can classify the kind of action taken more precisely, thus avoiding abuses and injustices against activists.

Key words: Digital Activism; Hacktivismo; Information Society; Internet.

1. INTRODUÇÃO

Este artigo tem por objetivo analisar o conceito de *hacktivismo* na Sociedade da Informação, de forma a melhor entender esta tendência e analisar sua possível aproximação com as práticas de desobediência civil. São escassas as fontes doutrinárias que possibilitam um aprofundamento do tema, forçando a conceituação a ser desenvolvida a partir quase que exclusivamente de textos da mídia tradicional e por meio das discussões entre os próprios ativistas. Não é incomum o foco da mídia sobre indivíduos que podem ser denominados como *hacktivistas*. O mundo tem sido inundado por relatos que colocam em evidência a fragilidade do sigilo de dados e a inexistência de privacidade nas redes sociais. Dentre esses casos, são destacadas a divulgação de dados secretos pela *WikiLeaks*; as polêmicas sobre Julian Assange e Edward Snowden que levaram à exposição das estratégias de espionagem e vigilância nos Estados Unidos da América; as ações do controverso *Anonymous*, entre outros. Não obstante, nos meios acadêmico este assunto ainda é tratado de forma incipiente.

Incumbir apenas para a mídia a classificação do *hacktivismo* representa o risco de que seja feita de forma superficial, com escassa base científica, potencializando futuros entraves se, porventura, a regulação desta atividade se fizer necessária. Assim, como o direito de manifestação e a desobediência civil, atos de rebeldia são em maioria narrados com paixão, mas a partir de pouca análise. Necessário que a comunidade acadêmica se antecipe com o escopo de tratar de forma mais precisa fenômenos como esse, sobre os quais pairam ânimos que levam à opacidade. Desse modo, cumpre definir o termo *hacktivismo* e conhecer como aqueles que o praticam costumam agir. Para tanto, foram compilados artigos acadêmicos disponíveis sobre o tema para, em seguida, pesquisar as principais formas de atuação dos *hacktivistas*. Assim, o artigo traça uma análise histórica do desenvolvimento das técnicas de ativismo hacker, buscando superar uma linguagem hermética presa a tecnicismos, para possibilitar o entendimento daqueles que possuem escasso conhecimento da tecnologia informacional. O texto atribui especial atenção para os impactos que atos de ativismo hacker tenham causado, assim como as principais ações a ele atribuídas. Definido o conceito, feita a análise histórica, será então analisada a

possibilidade de aproximá-lo das práticas de desobediência civil. Por fim, o artigo empenha-se em compreender as motivações e objetivos principais dos *hacktivistas*, ainda que seus atos possam muitas vezes não obter os resultados desejados, sendo importante entender as causas que os levam a agir.

2. CONCEITOS: *HACKTIVISMO; HACKER E CRACKERS*

Notadamente na sua análise morfológica, a palavra hacktivismo refere-se a um amálgama das palavras hacker e ativismo[4], sendo importante, para a definição deste último termo (ativismo), o uso da força para fins políticos. *Hacktivismo* será, portanto, o uso da força para exercer fins políticos utilizando-se de conhecimentos de informática. A definição de *hack* pode ser explicada como "uma tentativa de usar a tecnologia de uma maneira original, não ortodoxa e inventiva"[5]. Uma análise morfológica leva o leitor a crer que o *hacktivismo* limita-se à informática, entretanto, seus efeitos já são sentidos aquém do espaço digital. Esse termo poderia ser definido, ainda, como "o uso não violento de ferramentas ilegais ou legalmente ambíguas em busca de fins políticos " (SAMUEL, 2004, p 2). Fora em 1996 que o termo *hacktivismo* seria utilizado pela primeira vez, através de um hacker conhecido por "Omega" que se passou a denominar como tal o *"hacking"*, ação com o intuito de atingir fins políticos. Seria nas discussões de um grupo hacker intitulado *"Cult of the Dead Cow – CDC"* que o termo se popularizaria. Os mais diversos grupos viriam a buscar a justificativa de seus atos, através de um debate sobre a ideologia *hacktivista* e há registros de que teria sido um membro conhecido por *"Reid Fleming"* que viria a traçar o paralelo entre *hacktivismo* e a Declaração Universal dos Direitos Humanos, em especial no artigo XIX:

> Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

[4] Hacker, de acordo com o dicionário Michaelis, trata-se de "(réker) (ingl) sm Inform Pessoa viciada em computadores, com conhecimentos de informática, que utiliza esse conhecimento para o benefício de pessoas que usam o sistema, ou contra elas. " (MICHAELIS, 2015). Ativismo, ainda utilizando o mesmo dicionário será "sm (ativo+ismo) 1 Filos Acentuação da atuação consequente da vontade, na formação da cultura e da sociedade; toda criação espiritual, bem como a arte e a teoria científica devem servir à atividade dirigida a uma meta. 2 Doutrina ou prática de dar ênfase à ação vigorosa, p ex, ao uso da força para fins políticos." (MICHAELIS 2015)

[5] "[...] the hack is more widely defined as an attempt to make use of technology in an original, unorthodox and inventive way." (TIM JORDAN, 2004,p 6). Tradução pessoal, assim como todas as demais.

Apesar de a Declaração Universal dos Direitos Humanos ter fornecido uma base moral, ainda não seria o suficiente para pressionar os mais diversos países a aceitar o *hacktivismo* como forma de manifestação. Através de sugestão de Cindy Cohn, na época advogada especializada em direito digital, atualmente diretora jurídica do Eletronic Frontier Foundation, que os grupos em análise adotariam como base legal de sua luta o Pacto Internacional sobre os Direitos Civis e Políticos, artigo 19°, Parágrafo 2°:

> 2. Toda e qualquer pessoa tem direito à liberdade de expressão; este direito compreende a liberdade de procurar, receber e expandir informações e ideias de toda a espécie, sem consideração de fronteiras, sob forma oral ou escrita, impressa ou artística, ou por qualquer outro meio à sua escolha.

Foi baseado neste conceito jurídico moral que, em 4 de julho de 2001, seria publicado pelo portal Hacktivismo.com, a Declaração do *Hacktivismo*. Nessa Declaração viriam a ser incorporados elementos de ambos os documentos, acima referidos, denotando um amadurecimento nessa ideologia. Passaram o ser suas missões primordiais a defesa da liberdade de expressão e garantia do acesso à informação. Nessa Declaração do *Hacktivismo*, ocorre a mudança do ativismo indireto para um caráter de extremo confronto, "[...]que iremos estudar meios e formas de contornar a censura da internet, exercida pelo Estado, e implementaremos tecnologias capazes de desafiar violações no direito à informação"[6] (HACKTIVISMO.COM, 2001).

Esta mudança de postura, entretanto, ocasionou o surgimento de *hacktivistas* radicais, realizando atos que mais danificavam a imagem da prática do que colaboravam nas suas missões. Esta situação chegaria ao limite, quando em 1999 um grupo de ativistas conhecidos por *Legion of the Underground (LoU)*, declarou *cyberguerra* à China e ao Iraque, alegando que não mediriam esforços para destruir as redes de computadores desses países. Como forma de demonstrar seu poderio, o grupo invadiu o site governamental de Direitos Humanos da China. Temendo um incidente internacional e a retaliação contra a comunidade hacker, foi publicada uma declaração conjunta dos principais grupos *hacktivistas* à época, condenando a ação do *Legions of the Underground*. Seria através deste evento que o movimento se consolidaria, criando regras que tornariam obsoletas certas práticas da comunidade, formando assim um contexto mais civilizado para suas ações (RUFFIN, 2004, p 3).

[6] "that we will study ways and means of cirvumventing state sponsored censorship of the internet and will implement technologies to challenge information rights violations. " (hacktivismo.com, 2001)

Há uma distinção, segundo Alexandra Whitney Samuel, entre *hacktivismo* e ato político que pode ser feita de maneira tática, principiológica e cultural. A distinção tática reside no fato de que são usadas ferramentas diretas e transgressivas, acreditando que táticas de confronto são mais eficazes do que as convencionais. Distinguem-se de *cyber terroristas*, pois suas atitudes buscam o bem-estar humano. Culturalmente, distinguem-se de hackers pois acreditam que suas habilidades devem servir para um fim social (SAMUEL, 2004, p 246). Existem, entretanto, correntes que entendem o propósito do *hacktivismo* como uma desculpa para criar transtornos, e que a consequência destes atos será a intensificação dos regulamentos de internet. Eva Dadok descreve *hacktivismo* como "um novo movimento para expressar o desapontamento de alguém com algo (geralmente ideias políticas) ao quebrar o site de seu oponente e seu sistema de e-mails"[7](DADOK, 2005, p 2). Este conceito, apesar de distinguir *hacktivistas* de *crackers*, ao citar o ideal político por trás dos ataques, não permite a distinção real entre *hacktivista*, *hacker e cracker*, as práticas citadas são exatamente aquelas condenáveis pelos próprios *hacktivistas*. Essas conceituações, assim como suas distinções, serão tratadas mais adiante no artigo.

Para a compreensão do *hacktivismo* é necessário estudar a comunidade da qual surgiu. Ainda envolta em mistério, informações errôneas e romantizadas levaram a comunidade hacker a ser percebida, ora como bandidos, ora como *nerds*, ambos com fortes traços antissociais. Esta mistificação se deve à própria segregação da comunidade digital, dotada de regras e maneirismos internos que tornam hostil o ambiente àqueles que não o conhecem. A cultura hacker é fortemente baseada em humor e sarcasmo, com princípios únicos aos seus membros. Em seu livro *"The Hacker Ethic and the Spirit of the Information Age"*, Pekka Himanen explica que a comunidade hacker preza, acima de valores financeiros, a possibilidade de trabalhar em algo que trará reconhecimento dos demais membros e que seja de valor para a comunidade (HIMANEN, 2001, p 47).

O mundo dos hackers é dividido em comunidades, cada qual específica em sua temática, desde comunidades para programadores, cada linguagem de programação tendo sua, assim como de acordo com a intenção de cada hacker. O reconhecimento dentro da comunidade é de tamanha importância para os hackers que existe um jargão específico

[7] "It is a new movement of expressing someone's disappointment with something (usually it has to do with political ideas) by breaking into opponents websites or e-mail system." (EVA DADOK, 2005,p 2)

para membros que conquistaram o respeito dos demais através de seus conhecimentos técnicos, sendo denominados *wizards*, ou magos.

São denominados crackers aqueles que utilizam seu conhecimento para detectar vulnerabilidades no sistema e as utilizam para ganho pessoal. O termo foi criado por Richard Stallman (em seu artigo *On Hacking*, admite ter começado a usar o termo na década de 80), como forma de diferenciar estes indivíduos dos demais hackers da comunidade. Entre as atividades de cracker está a violação da privacidade, o furto de informações, além de atos de vandalismo e de chantagem. Existe, entretanto, uma forma mais branda de cracker, denominada *Grey hat*, que localiza falhas de segurança que podem ser utilizadas por crackers para causar dano e as expõem de forma a forçar a correção destas falhas por parte de seus desenvolvedores.

Este termo – *craker*, ganha principal importância quando observado em contraposição ao *hacktivismo*. Sua diferença, entretanto, reside no fato de que o ativismo hacker, apesar de por vezes ilegal e danoso, resguarda-se em um cunho moral, dotado de uma finalidade maior. As atividades exercidas por cracker, por vez, almejam o ganho pessoal, podendo ser financeiro ou sob forma de um duvidoso entretenimento.

3. EVOLUÇÃO HISTÓRICA E AÇÕES DE ATIVISMO HACKER

Seguindo a linha de Tim Jordan e Paul Taylor, pode-se classificar *hacktivismo* através de gerações, devido às características marcantes de cada momento (JORDAN, 2004, p 10). Certas práticas, apesar de não serem denominadas como *hacktivismo* à época, tiveram todas as características necessárias para que fossem assim denominadas. Deve-se ressaltar que, a mudança de uma geração à outra não significa que as práticas da geração passada tenham sido abandonadas. As gerações refletem mais o momento histórico em que se encontravam do que as técnicas utilizadas. Existe, entretanto, uma evolução técnica, que decorre dos avanços tecnológicos.

Ainda segundo Jordan, a primeira geração de ativistas desta modalidade é marcada pela ênfase no *hardware*. Surge com o desejo de cientistas e inventores na democratização da tecnologia. Não há uma agenda política definida nesta geração, seus atos, apesar de terem sido essenciais para a formação da sociedade moderna, foram praticados com objetivo de proporcionar melhorias para a sociedade como um todo.

A criação dos primeiros computadores pessoais, ou PCs, pode ser atribuída ao desejo da democratização da tecnologia. Criado pela família e companhia Olivetti, o *Programma 101*, considerado por muitos o primeiro computador pessoal do mundo, tinha por intenção inserir pequenas empresas à computação, custando em seu lançamento 1/10 do valor dos computadores *mainframe* utilizados na época. Seu sucesso não foi devido apenas ao valor, mas também por ser não maior que uma máquina de escrever e por não ser necessário refrigeração constante para que funcionasse (VEGTER, 2009).

Não apenas os computadores pessoais, mas a própria criação da internet poderia ser atribuída aos *hacktivistas* da primeira geração. Segundo Bruce Sterling (STERLING, 2015), o governo americano teria criado a rede que daria origem à internet por temer um ataque nuclear. O problema residia no fato de que, caso houvesse um ataque, os cabos e postes de comunicação estariam vulneráveis aos danos da explosão, desabilitando assim a comunicação. Para resolver este dilema foi criado um sistema denominado ARPANET, que visava descentralizar a comunicação, utilizando supercomputadores como nós de rede, que processariam os dados enviados de maneira separada, garantindo que a informação chegaria a seu destino. Em 1969, o primeiro nó foi criado em UCLA, e antes do final do ano a rede já era integrada por quatro nós. Em 1972 a rede já contava com trinta e sete nós. Curiosamente, a maneira que esta rede foi utilizada foi completamente diferente da prevista por seus idealizadores. Ainda de acordo com Sterling, os usuários estavam tratando esta rede como um correio de longa distância, utilizando-a para trocar dados de pesquisa, contribuições, e até mesmo conversas pessoais.

Em 1977, a rede conhecida como ARPANET passou a adotar o novo protocolo TCP/IP, que, por ser de domínio público, passou a permitir o ingresso de maior variedade de máquinas à rede, vindo a substituir completamente a rede original, dando origem então à conhecida INTERNET. A rede ARPANET foi oficialmente extinta em 1989, totalmente substituída pela INTERNET e o protocolo TCP/IP. Apesar do cunho social destes projetos, já nesta época havia outros movimentos que já começavam a exercer pressão política com o uso da tecnologia. Conforme Tim Jordan (JORDAN, 2004, p 13), foi com o boletim informativo do *Youth International Party Line* (YIPL) que ficou marcado a presença da tecnologia em manifestação política. Esses movimentos usavam de seu boletim para fazer duras críticas à guerra do Vietnã, em especial sobre a taxação de contas telefônicas para o auxílio nos esforços de guerra. Quando as denúncias feitas por este grupo se mostraram

infrutíferas, foi desenvolvida outra tática para continuar a pressão política. O grupo passou então a se chamar *Technological American Party*, e utilizou a estrutura do boletim informativo para disseminar técnicas que permitiam realizar ligações telefônicas gratuitamente, evitando assim contribuir para a guerra.

Esta segunda geração de *hacktivistas* realiza suas manifestações políticas não de forma tradicional, como ativistas ou partidos o fazem, mas pelo próprio *hack* em si. Sua transgressão é feita pois, em sua busca por conhecimentos que acabam rompendo paradigmas sociais que não haviam sido tocados desde então. Estavam neste momento, percebendo que seus atos tinham repercussões político-sociais e que causavam impactos na lei. Devido à suas inclinações, estes *hacktivistas* utilizavam meios inteligentes de ultrapassar limitações, o que por vezes acabava pela infração da lei ou por seu ato se encontrar em um vácuo legal, vez que a legislação raramente acompanha a criação tecnológica, principalmente tratando-se da vanguarda digital.

No início da era digital, a programação utilizada para desempenhar funções nos computadores era compartilhada de maneira livre, não havia licença ou legislação que ditasse a maneira como esses programas seriam compartilhados. Seu acesso era através da comunidade digital e de forma livre e desimpedida, podendo o usuário alterar o código do programa para adaptá-lo à sua utilização. Essa prática, entretanto, foi alterada em 1980 quando o Congresso Norte-Americano adicionou em sua legislação a definição de "programa de computador", permitindo que fosse submetida ao sistema Copyright. A mudança ao sistema Copyright fez com que, obrigado a lidar com a burocracia que o seguiu, e pela necessidade de acordos de distribuição e marketing, apesar de retentor do direito do software, os autores deixariam de receber o fruto de seu trabalho, colhido pelas distribuidoras (ST. LAURENT, 2004, p 4).

Foi com Richard Stallman, em seu projeto GNU / Linux (trata-se de um Sistema Operacional e uma coletânea de softwares criados para o público geral) que se deu a brusca mudança na forma como seria protegida a propriedade intelectual produzida pela comunidade hacker. O projeto GNU surge do espírito de solidariedade de seus idealizadores, em compartilhar programas desenvolvidos com demais usuários. A licença criada então pelo projeto GNU visava não apenas a distribuição gratuita dos programas desenvolvidos, bem como permitir sua modificação e redistribuição, limitando apenas que as modificações criadas fossem também ser distribuídas de forma gratuita e livre. A

criação desses softwares é feita com base em contribuições espontâneas, seja na forma financeira ou de equipamentos, ou através de trabalho voluntário. Baseado no projeto GNU, surge um movimento que visa a criação de novas licenças que adaptem as necessidades dos desenvolvedores, enquanto permitem novas tecnologias baseadas nas criações sob sua proteção, este movimento foi denominado Copyleft, em uma nítida sátira à legislação de propriedade intelectual Copyright (COLEMAN, 2012, p 40).

O movimento licença aberta que se iniciou no GNU deu origem a diversas outras licenças, com as mais variadas formas de limitação, seja na distribuição, seja na modificação, seja na patente, cada licença adaptando-se para uma finalidade específica. O ponto comum entre elas reside no fato de que todas disponibilizam o código para que seja estudado por demais hackers, propagando assim a liberdade de informação. Essas licenças não obrigam o usuário a aceitá-las, entretanto, a negativa de seu aceite implicaria na aceitação da licença padrão, a conhecida Copyright, o que não permitiria seu uso, modificação ou distribuição. Baseada nessa premissa é que foi criada a licença *hacktivista* "HESSLA – *Hacktivismo Enhanced-Source Software License*". A denominada HESSLA foi produzida por *Oxblood Ruffin* em conjunto com o advogado Eric Grimm. Ela permite a utilização, modificação, distribuição do software sob sua licença, vetando, entretanto, o uso para a violação de direitos humanos e que sejam adicionados ao código funções que permitam a identificação e espionagem de seus usuários. A principal crítica, quanto a essa licença, está na alegação de que violadores de Direitos Humanos não estariam ameaçados por licenças, entretanto, pela maneira ao qual a licença foi escrita, sua violação implicaria na possibilidade de atuação do governo Norte-Americano, o que levou as dúvidas quanto a sua aplicabilidade a serem aplacadas (RUFFIN, 2004).

Com o crescente acesso à internet, a privacidade de seus usuários passou a ser um tema em foco na comunidade hacker. Não apenas pela ameaça constante da invasão de seus dados pessoais por outros usuários com intenções não identificadas sendo que esses dados também poderiam ser facilmente acessados por agências do governo e até mesmo pelo provedor de acesso. Como forma de limitar o acesso a esses dados foram criados diversos programas para proteger a privacidade na internet. Desenvolvido por Philip Zimmermann, o PGP, ou *Pretty Good Privacy*, é um programa de encriptação de dados criado em 1991, com o intuito de mascarar o conteúdo visualizado no computador. De acordo com seu criador, "criptografia permite o usuário garantir sua privacidade com as

próprias mãos” [8]. O temor não está apenas na possibilidade de o Estado interceptar dados pessoais, mas também rivais de negócios, usuários maliciosos, crime organizado e até mesmo nações estrangeiras. Este temor se concretizaria anos após com a denúncia de Edward Snowden, de que a Agência de Segurança Norte-Americana, NSA, estaria com dados de acesso dos mais diversos usuários por todo o mundo, incluindo líderes mundiais e representantes oficiais de governos estrangeiros. A criptografia, entretanto, passou a ser utilizada como forma ativa de protesto, seu uso permitia a comunicação com outros usuários que estavam acessando a internet através de redes limitadas por censura estatal. Assim, iniciava-se com a criptografia o *hacktivismo* direto, de confronto (RUFFIN, 2004).

Em 2002, na feira hacker CodeCon, o grupo de ativistas *“Cult of the Dead Cow”* publicou o programa *“Peekabooty”* que alegava, como intuito, utilizar criptografia para driblar as restrições de acesso à internet impostas por governos tiranos como o da Arábia Saudita e da China. Esse programa utilizava da criptografia e de redirecionamento de sites para impedir que o Estado identificasse tanto o site acessado quanto o usuário que requisitou seu acesso. Com o sucesso do programa *“Peekabooty”*, o grupo passa a trabalhar em um projeto complementar, que visava burlar não apenas as restrições de acesso à internet como também os filtros de palavras utilizados por esses governos para impedir a visualização de assuntos relacionados aos Direitos Humanos, visões políticas críticas, notícias produzidas em jornais situados fora da soberania nacional e diversos assuntos que poderiam incentivar desobediência. Foi criado então um programa criptográfico chamado “*Camera/Shy*” que permitia aos seus usuários permear informações dentro de imagens, que seriam consideradas inofensivas por esses filtros, em uma nítida forma de esteganografia digital. Como forma de permitir o download destes programas através das redes censuradas foi criado um programa denominado *“Six/Four”*, sendo o nome uma alegoria à data do massacre da praça da Paz Celestial. Seu funcionamento consistia na junção dos dados de aplicações possibilitando seu ocultamento através e qualquer protocolo de internet. Seriam estas contribuições que culminariam na criação da licença HESSLA (descrita anteriormente), como uma tentativa de vetar seu uso indevido. Outra forma de criptografia com o intuito de mascarar o usuário foi desenvolvido o browser conhecido por Tor. Este browser foi financiado pela *EFF – “Electronic Frontier Foundation*”, uma ONG internacional que advoga pelos direitos digitais, criada em 1990,

[8] “PGP empowers people to take their privacy into their own hands.” (ZIMMERMANN, 1991,p 3)

fornece suporte legal e promove a ligação entre *hacktivismo* digital e o ativismo tradicional.

A verdadeira arma do ativismo criptográfico, entretanto, veio com o site *Wikileaks*, de Julian Assange. Seu funcionamento se dá através de um site vinculado a uma equipe de jornalistas, hackers e advogados, cuja função é receber denúncias anônimas e documentos comprovando essas denúncias para expor ações moralmente incorretas de empresas, governos e funcionários públicos. Para garantir o anonimato de seus denunciantes o *Wikipedia* conta com "um drop box anônimo de alta segurança, fortificado com tecnologias criptográficas de última geração" (WIKILEAKS.ORG, 2011)[9].

Por manter o anonimato, o site *Wikileaks* recebe documentos e denúncias constante, alguns dos quais já figuraram na mídia tradicional expondo atrocidades cometidas pelo governo Norte Americano durante as invasões do Iraque e do Afeganistão. Entre esses documentos encontra-se o famoso vídeo de um helicóptero abatendo civis em Nova Bagdá, em 12 de julho de 2007. Entre as vítimas civis, havia dois jornalistas do jornal Reuters. Esse vídeo ficou conhecido como Ataque aéreo de Bagdá e conjuntamente com diários de guerra do Afeganistão e do Iraque compôs o acervo de documentos que os jornais The Guardian, New York Times e Der Spiegel expuseram como forma de demonstrar as atrocidades cometidas e o nítido descaso aos direitos humanos durante tais invasões.

Foi também exposto pelo *Wikileaks* o episódio que ficou conhecido como *"Cablegate"* onde foram expostos diversos documentos da diplomacia norte-americana demonstrando o suporte do governo a ditaduras, espionagem de membros da ONU, tráfico de influência, chantagem, entre outros temas que demonstram falhas morais e éticas do governo. Esses documentos continham, também, detalhes sobre o funcionamento da Prisão da Baía Guantánamo, onde são descritas práticas consideradas violações dos direitos humanos, como tortura e as más condições a que os prisioneiros estavam sujeitos.

Em resposta aos documentos expostos, foi instituído embargo bancário ao *Wikileaks* sob a alegação de que suas atividades seriam ilegais e os principais meios de doação do site passaram a bloquear as transações. Entre as instituições financeiras que se recusam a receber quantias doadas ao *Wikileaks* estão a Master Card, Visa, PayPal e o Bank of America (ASSANGE, 2013 p 39). Este bloqueio tem sido driblado através de

[9] "Unlike other outlets, we provide a high security anonymous drop box fortified by cutting-edge cryptographic information technologies." (WIKILEAKS.org, 2011)

acordos entre a Fundação Wau Holland, a Fundação "Freedom of the Press", para processamento de doações voltadas à manutenção do *Wikileaks*, além do uso de Bitcoin e Litecoin, moedas digitais com valor real (https://shop.wikileaks.org/donate).

4. DESOBEDIÊNCIA CIVIL DIGITAL

Desobediência civil é o termo usado para designar "[...] o direito de recusar obediência ao governo, e de resistir a ele, quando sua tirania ou sua ineficiência são grandes e intoleráveis". (THOREAU, 2012, p 11). Pelo conceito de desobediência civil, o governo que deveria representar o desejo da maioria por vezes é composto por uma elite política, realizando atos que questionam a moral de seus subordinados. Constituiria desobediência civil quando, obrigado pelo Estado, o cidadão abstém-se de agir, como forma de protesto. Nem todos os casos de legislação injusta devem ser resolvidos através de desobediência civil. Propõe John Raws, em sua obra *A Theory of Justice*, que os casos que necessitam de tal medida sejam aqueles para os quais os caminhos tradicionais de reivindicar já tenham sido tomados sem sucesso, quando protestos legais e outras demonstrações restaram infrutíferas (RAWLS, p 326). Assim, a desobediência civil deverá ser usada apenas em casos de sérias violações à noção de justiça. Propõe ainda, que a desobediência civil seja praticada de maneira a não ocasionar a destruição da lei e da Constituição. Discute Rawls, que fica difícil a aplicação tal conceito, vez que o protagonista da violação moral em sua maioria é o próprio Estado e este o faz em desacordo com a sua própria lei e Constituição, entendendo-se como necessário, nos casos de desobediência civil um balanço entre a lei que será quebrada e a moral a ser defendida. Segundo Maria Garcia a desobediência civil deve ser um ato inovador acima de ser um ato destruidor: "A desobediência civil pode-se conceituar como a forma particular de resistência ou contraposição, ativa ou passiva do cidadão, à lei ou ato de autoridade, quando ofensivos à ordem constitucional ou aos direitos e garantias fundamentais, objetivando a proteção das prerrogativas inerentes à cidadania" (GARCIA, 2003, p 18).

A mentalidade da desobediência civil eletrônica é semelhante à da forma tradicional. Reside na resistência a um Estado abusivo através do não cumprimento da lei. A forma de resistência, entretanto, traz grande controvérsia entre *hacktivistas*. Argumentando o coletivo artístico "*Critical Art Ensemble*" que: "Bloquear a entrada de um edifício, ou outra forma de resistência no espaço físico pode evitar sua reocupação

(circulação de pessoas), mas isto terá poucas consequências enquanto o capital-informativo continuar a circular”[10]. Através deste argumento, grupos de *hacktivistas* justificam o uso de táticas como “*Denial of Service*”[11], ou “*Web-defacing*”[12]. Surge, entretanto, um conflito ideológico. Tais táticas seriam uma afronta à liberdade de expressão, um dos pilares do *hacktivismo*. Segundo Oxblood Ruffin, membro do “*Cult of the Dead Cow*”, “[...] não há diferença entre desabilitar a habilidade do servidor Web de prover informações – ainda que desagradáveis – e gritar com alguém em uma audiência pública até que esta pessoa se cale ” [13]. Divide-se então a desobediência civil eletrônica em duas formas distintas. Há argumentação de que, por se tratar de uma forma digital de desobediência civil, é não violenta por natureza, já que não ocorre confrontos físicos com nenhuma das partes envolvidas. A principal tática adotada pelos defensores desta argumentação é a de violar a rede e bloquear o fluxo de informação, causando assim impactos econômicos que resultariam em pressão suficiente para forçar uma mudança. No entanto, a desobediência civil eletrônica pode ser feita de uma maneira mais “civilizada”, através do combate tecnológico da censura e no acesso à informação. Este método de pressão pode verter resultados satisfatórios, apesar de que muitas vezes a informação a ser distribuída vai contra o interesse governamental. Este caso pode ser facilmente ilustrado na mídia com o vazamento de documentos pelo *Wikileaks* e as denúncias do soldado Bradley Manning[14], ou até mesmo com a denúncia feita por Edward Snowden. Tais atos encaixam-se com a definição de Henry Thoreau sobre desobediência civil: “Não é a obrigação de um homem, evidentemente, dedicar-se à erradicação de um mal qualquer, nem mesmo do maior que exista; ele pode muito bem ter outras preocupações que o absorvam. Mas é seu dever, pelo menos, manter as mãos limpas e, mesmo sem pensar no assunto, recusar o apoio prático ao que é errado. ” (THOREAU, 2012,p 15)

[10] “Blocking the entrances to a building, or some other resistant action in physical space, can prevent reoccupation (the flow of personnel), but this is of little consequence so long as information-capital continues to flow.” (CRITICAL ART ENSEMBLE, 1996,p 9)
[11] Trata-se de tática onde um computador realiza múltiplas conexões em um servidor, visando utilizar sua capacidade em totalidade, impedindo assim que outros usuários o acessem.
[12] Outra tática empregada onde o invasor obtém acesso ao domínio onde está hospedado o site e altera a sua composição, com o intuito de que quem o acesse veja a mensagem do invasor e não a original do proprietário do site.
[13] “There isn't a whole lot of difference between disabling a Web server's ability to provide information - even if that information is distasteful - and shouting down someone in a town hall meeting. ” (OXBLOOD RUFFIN, 2004,p 3)
[14] Soldado Bradley Manning é atualmente conhecido por Chelsea E. Manning, após trocar sua identidade de gênero, foi o responsável pela exposição dos documentos que culminaram no escândalo conhecido pela mídia por “Cablegate”

Não há dosimetria adequada para a punição estatal ao *hacktivismo*, quando levados aos tribunais, sendo as penas as mais variadas, e em muitos casos a punição é aplicada antes que chegue ao tribunal. As acusações contra os ativistas vão de "comprometimento não autorizado de computador protegido" até cyber terrorismo e espionagem. Partindo do princípio de que *hacktivistas* são manifestante praticando desobediência civil, certas condenações se tornam extremadas e contrárias aos Direitos Humanos e ao Pacto Internacional dos Direitos Civis e Políticos.

Pode-se conferir a penalização abusiva aos ativistas ao analisar o caso de Aaron Swartz, criador do grupo *"Demand Progress"* que combateu a legislação norte americana SOPA ("*Stop Online Piracy Act*") e PIPA ("*Protect Intelectual Property Act*"). Ele foi um dos principais grupos a defender a neutralidade da internet. Sendo indiciado e enfrentando a possibilidade de passar 50 anos retido, Aaron Swartz cometeu suicídio. Fortes indícios levam a crer que o suicídio foi causado pela agressão dos Procuradores envolvidos no caso ao tentar penalizar o *hacktivista*. O crime cometido foi ter utilizado um programa para fazer o download de textos acadêmicos e disponibilizá-los online, livre de custos. Não apenas Aaron Swartz sofreu pelo hábito de "fazer de exemplo" usado pela Procuradoria norte americana para punir ativistas, mas o caso de Bradley Manning também pode ser citado. Utilizando a plataforma *Wikileaks*, o soldado Bradley Manning, agora conhecido por Chelsea Manning, relatou diversos abusos cometidos pelo militarismo norte americano com as invasões do Iraque e do Afeganistão. Além dos documentos de guerra, Bradley Manning revelou documentos da diplomacia norte americana que demonstravam abusos cometidos por seus funcionários. Após passar três anos detido sem julgamento, foi indiciado sob o *Espionage Act* e julgado sem direito a utilizar como defesa o interesse público em receber a denúncia. Sua pena foi de trinta e cinco anos, considerada por especialistas como forma do governo americano de demonstrar que denúncias não serão toleradas (ASSANGE, 2013, p 12).

Tal política de não tolerância a denúncias também pode ser observada no caso de Edward Snowden, antigo empregado da Agência Nacional de Segurança norte americana (NSA), responsável pela denúncia de que a agência teria um programa de vigilância em massa, incluindo a vigilância sem autorização judicial e a vigilância de políticos e figuras de interesse de países aliados. Indiciado por "comunicar informação de defesa nacional de

maneira não autorizada" e "voluntariamente revelar comunicação secreta de inteligência", também no *Espionage Act*, que não permite a ampla defesa dos acusados.

A desobediência civil eletrônica ganha importância ao se analisar o Tribunal de Nuremberg, onde as atrocidades cometidas pelo regime nazista foram rebatidas por aqueles que as cometeram como lhes sendo obrigatórias em razão da lei vigente à época. No entanto, sob o prisma moral a desobediência civil torna-se forçosa, principalmente em casos onde ocorre violação dos direitos humanos, como, evidentemente, foi o caso do nazismo durante a Segunda Guerra Mundial.

5. CONSIDERAÇÕES FINAIS

A cultura hacker, formada principalmente por pessoas que buscam conhecimentos por natureza, proporcionou, ainda que de maneira espontânea, palco para discussões de cunho político, estas muitas vezes culminaram em ação, encabeçada pelos membros dessa cultura hacker. Esses grupos visam mudança na política mundial, munidos de ideais nobres e conhecimento tecnológico, ainda que em pouco número são capazes de exercer forte pressão visando mudanças. Por tratar-se de cultura baseada na meritocracia, as ações *hacktivistas* costumam acontecer com mais facilidade que o ativismo tradicional. Identificando um problema o hacker tende a pensar em formas criativas de solucioná-lo, independente do impacto que sua criação irá gerar. Essa natureza inerente ao hacker o coloca na posição de agente de mudanças, ainda que acidentais.

Há um conceito errôneo sobre o que seria um hacker, sendo marcado pela mídia tradicional como criminoso, perseguindo senhas de banco e roubando dados. Em realidade, o hacker é uma pessoa dotada de curiosidade e solucionador de problemas. Não há que se negar a existência daqueles que utilizam a informática para ações criminosas, entretanto, estes indivíduos não fazem parte da comunidade hacker, sendo inclusive marginalizados nesta. A comunidade *hacktivist*a, no entanto, pode vir a violar leis para cometer atos em defesa de um bem maior. A liberdade de expressão e o livre acesso à informação costumam ser os princípios motivadores de seus atos, entretanto, outros princípios também são defendidos, como a privacidade e o combate à tortura.

É necessária a criação de mecanismos de defesa do *hacktivista*, a legislação existente permite que seus atos sejam julgados de forma extremista, pois foi criada em

tempos de guerra, fato este que exigia um maior rigor nas punições. Ausente a guerra, nada justifica a maneira como esses casos são conduzidos e tratados, violando princípios essenciais a um Estado de direito, cabendo aos operadores do direito corrigir tais abusos de forma a se punir apenas as ações verdadeiramente criminosas sem sacrificar o direito à manifestação e sem comprometer a luta por direitos, liberdade e ética nas relações sociais de um modo geral e do Estado com a sociedade.

REFERÊNCIAS:

ASSANGE, JULIAN. **Cypherpunks:** liberdade e o futuro da internet; tradução Cristina Yamagami, 1ª ed. – São Paulo, Boitempo, 2013.

BARBOSA, Marco Antonio. Poder na Sociedade da Informação. In: PAESANI, Liliana Minardi (coord.). **Direito na sociedade da informação.** São Paulo: Atlas, 2007

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

_____. Abordagens recentes da pesquisa jurídica na Sociedade da Informação. In: PAESANI, Liliana Minardi (coord.). **Direito na sociedade da informação V. 2.** São Paulo: Atlas, 2009.

_____. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells.. In: DE

COLEMAN, GABRIELLA. **Coding Freedom:** The Ethics and Aesthetics of Hacking. Princeton University Press, 2012.

COLEMAN, GABRIELLA. The (Copylefted) S**ource code for the ethical production of information freedom**. Nova Delhi, Sarai: The New Media Initiative, 2003.

CRITICAL ART ENSEMBLE**. Electronic civil disobedience & other unpopular ideas**. New York, Autonomedia, 1997.

DADOK, EVA. **Hacktivism:** A Free Form of Expression or Digital Vandalism? Bethesda, SANS Institute.

GARCIA, MARIA. **A desobediência civil como defesa da Constituição**. São Paulo: Revista Brasileira de Direito Constitucional n° 2, 2003.

HACKTIVISMO.COM. **The Hacktivismo Declaration**, 2001. Disponível em: < http://www.hacktivismo.com/public/declarations/en.php> acessado em: 10/10/2015

HIMANEN, PEKKA. **The hacker ethic:** a radical approach to the philosophy of business. 1ª ed. New York, Random House, 2001.

JORDAN, TIM; TAYLOR, PAUL. **Hactivism and cyberwars: rebels with a cause**. 1ª ed. New York, Routledge, 2004.

RAWLS, JOHN. **A theory of justice**. Rev. ed. Harvard University Press, 1999.

RUFFIN, OXBLOOD. **Hacktivism, from here to there**, 2004. Disponível em: < http://www.cultdeadcow.com/cDc_files/cDc-0384.php> acessado em: 11/10/2015

SAMUEL, ALEXANDRA WHITNEY. **Hacktivism and the future of political participation**. Cambridge, Harvard University, 2004.

ST. LAURENT, ANDREW M. **Understanding open source and free software licensing.** 1ª ed. Sebastopol, O'Reilly Media, 2004.

STALLMAN, RICHARD. **Linux and the GNU System**. Disponível em: < https://www.gnu.org/gnu/linux-and-gnu.html> acessado em: 13/10/2015

_____. **The GNU Manifesto**, 1985. Disponível em: < http://www.gnu.org/gnu/manifesto.en.html> acessado em: 13/10/2015

_____. **On hacking**. Disponível em: < https://stallman.org/articles/on-hacking.html > acessado em 13/10/2015.

STERLING, Bruce. **INTERNET (aka a short history of the internet)**. Disponível em: <https://w2.eff.org/Net_culture/internet_sterling.history.txt> acessado em: 08/10/2015.

THOREAU, HENRY DAVID. **A desobediência civil;** tradução José Geraldo Coutor – São Paulo, Penguin Classics Companhia das Letras, 2012.

VEGTER, Wobbe. **Cyber heroes of the past:** Camillo Olivetti, 2009. Disponível em: <http://wvegter.hivemind.net/abacus/CyberHeroes/Olivetti.htm> acessado em: 08/10/2015

WIKILEAKS.ORG. **What is Wikileaks?**, 2011. Disponível em: <https://wikileaks.org/About.html> acessado em: 27/06/2016

ZIMMERMANN, PHILIP. **Why I wrote PGP**, 1991. Disponível em: < https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html> acessado em: 10/10/2015.