DOI: http://dx.doi.org/10.18315/argumentum.v8i3.13396

ARGUMENTUM

ARTIGO

Hacking político: crime cibernético ou manifestação legal de protesto?

Political hacking: cyber-crime or legal protest demonstration?

Bárbara Maria Farias MOTA[1]
Renato HAYASHI[2]
Antônio Alves Tôrres FERNANDES[3]

Resumo: O presente trabalho discute as controvérsias em torno de protestos online transgressivos (DDoS, Deface e Leak) a partir da atuação da rede hacktivista *Anonymous*. Diferentemente de outras formas de manifestações no ambiente virtual, esse tipo de intervenção – coordenada por indivíduos com expertise computacional – encontra-se na fronteira entre o que é ou não politicamente permissível e lícito. Frente a isso, são confrontadas as principais interpretações que permeiam esse debate, concedendo-se especial atenção à abordagem do tema pela legislação brasileira, que tipifica esses atos como delitos informáticos. Essa perspectiva contrasta com a compreensão de que essas ações são socialmente justificáveis como manifestações legais de protesto, a depender de seus propósitos. Este trabalho espera contribuir para os futuros debates acerca das novas táticas de ação na esfera pública interconectada e para o aperfeiçoamento da legislação brasileira sobre o tema.
Palavras-chave: Ciberespaço. Crime por computador - Brasil. Crime político. Hacker. Direito e informática - Brasil.

Abstract: This paper discusses the controversies around transgressive online protests (DDoS, Deface and Leak) from a case study of the hacktivism network Anonymous. Differing from other forms of demonstration in the virtual world, this type of intervention – coordinated by individuals with computer expertise - lies on the borderline of what is politically permissible and licit. The main interpretations related to this debate are addressed, giving special attention to the Brazilian legislative view on the issue, which typifies those acts as criminal offences. This perspective contrasts with the understanding that these acts are socially justifiable as legal demonstrations, depending on their purpose. Finally, this paper aims to contribute to future debates regarding new tactics in the interconnected public sphere and the improvement of Brazilian legislation on this matter.
Keywords: Cyberspace. Crime by computer - Brazil. Political crime. Hacker. Law and informatics - Brazil.

Submetido em: 19/6/2016. Aceito em: 20/11/2016.

[1] Mestranda em Sociologia e Bacharela em Ciências Sociais pela Universidade Federal de Pernambuco (UFPE, Recife, Brasil). Av. Prof. Moraes Rego, nº 1235, Cidade Universitária, Recife (PE), CEP. 50670-901. E-mail: <barbarafmota@gmail.com>.

[2] Professor e Coordenador de Pós-Graduação da Uninassau, Rua Guilherme Pinto, nº 114, Graças, Recife (PE), CEP. 50050-290 e da Faculdade Joaquim Nabuco, Av. Guararapes, nº 233, Santana, Recife (PE), CEP. 50010-460. Advogado e Assessor Jurídico da Câmara Municipal do Recife. Rua Princesa Isabel, nº410, Boa Vista, Recife (PE), CEP. 50050-450. E-mail: <professorrenatohayashi@hotmail.com>.

[3] Graduando em Ciência Política pela Universidade Federal de Pernambuco (UFPE, Recife, Brasil). Av. Prof. Moraes Rego, nº 1235, Cidade Universitária, Recife (PE), CEP. 50670-901. E-mail: <fernandes.anttonio@gmail.com>.

Leis injustas existem:
devemos nos contentar em obedecê-las?
Ou nos empenhar em aperfeiçoá-las, obedecendo-as até obtermos êxito?
Ou devemos transgredi-las imediatamente?

(Henry David Thoreau)

Introdução

As intensas transformações sociotécnicas ocorridas nas últimas décadas consolidaram a internet como um espaço estratégico para mobilização das demandas de diferentes grupos e segmentos sociais. Dessa forma, as redes interativas condicionam a sobrevivência, a deliberação e a expansão dessas mobilizações de modo autônomo e descentralizado. Nesse sentido, é justamente em tempos de poder nômade e de vigilância contínua que o uso do *hacking* de computador para fins políticos se intensifica, pois os hackers[4] conseguem executar ações de protesto disruptivas, embaralhando dados e apagando os seus rastros nas redes informacionais (SILVEIRA, 2009). Por outro lado, esses protestos se encontram na fronteira entre o que é ou não politicamente permissível e lícito. Logo, o *hacking* motivado politicamente é uma manifestação legal de protesto ou um crime cibernético? O objetivo deste trabalho é discutir as controvérsias presentes em torno da atividade de protestos transgressivos no âmbito digital, tais como o ativismo hacker, ora compreendido como manifestação legal de reivindicação, ora interpretado como crime cibernético. Para tanto, o estudo discute conceitualmente a natureza ambivalente do hacktivismo, dedicando especial atenção aos *softwares studies* e à visão da legislação brasileira em relação à questão.

O trabalho está dividido da seguinte forma: na primeira seção, discorre-se sobre a perspectiva que enquadra o hacktivismo como um tipo de desobediência civil eletrônica. Na segunda parte, é apresentada a ação hacktivista desenvolvida em território brasileiro, empreendida majoritariamente pela rede *Anonymous*. Na terceira seção, em contraposição à concepção do ativismo hacker enquanto ações legítimas de protesto, é destacada a perspectiva da legislação vigente no Brasil, que evidencia um enquadramento das táticas de hacking para fins de protesto (caso específico do *DDoS*[5] e *Deface*[6]) em crimes cibernéticos. Por fim, são trazidas as considerações finais do trabalho.

[4] O hacker aqui é compreendido como o indivíduo que utiliza os seus conhecimentos técnicos para fins políticos ou motivações éticas em contraposição ao cracker, que os utiliza para causar prejuízos (roubo de senhas de cartão de crédito, uso de *botnets* para lucro pecuniário, desenvolvimento de vírus computacional, etc.) e é enquadrado como cibercriminoso. Essa distinção foi feita justamente por hackers, na década de 1980, em contraposição à representação popularizada pelos *mass media* do hacker como sinônimo de criminoso.

[5] Acrônimo para *Distributed Denial of Service*, também conhecido por ação de negação de serviços. É a sobrecarga de um site proveniente de múltiplas entidades computacionais simultâneas esgotando a capacidade de processamento do servidor que hospeda a página. Tem similitude com um protesto na rua à medida que, como forma de contestação, ocupa e obstrui um espaço virtual impossibilitando outras pessoas de utilizá-lo.

[6] Também é conhecido como *grafiti online*. Por meio das falhas de segurança no servidor que hospeda um site, é possível ter acesso a esse servidor e alterar os arquivos que compõem a página no intuito de provocar modificações na sua aparência ou no seu funcionamento. O *deface* pode estar relacionado a uma motivação de cunho político, a exemplo da substituição da página do Ministério da Defesa do Governo da Síria, por um hacker, em protesto de apoio aos cidadãos do país em 2011.

1 Hackerativismo e a desobediência civil eletrônica

A ascensão dos protestos no ciberespaço se disseminou com a popularização da rede mundial de computadores na década de 1990. Uma das principais referências ao uso politicamente motivado da rede foi quando os zapatistas se valeram da Web para disseminação da sua luta, superando as fronteiras do México, sem a intermediação e restrição dos meios de comunicação comerciais – como a Televisa, estação de TV controlada pelo governo e campeã de audiência no país (CLEAVER, 1998). Outro exemplo notório ocorreu em 1999, quando das manifestações contra o encontro da Organização Mundial do Comércio (OMC), com adesão de ativistas em âmbito local e global, mobilizados por meio das redes digitais. *O mundo não está à venda* era o slogan em destaque da Associação pela Tributação das Transações Financeiras para ajuda aos Cidadãos (ATTAC) em contraposição à lógica mercadológica da globalização neoliberal que a OMC buscava instituir. Essas manifestações – igualmente conhecidas como *Batalha de Seattle* ou como *N-30* (MORAES; RAMONET; SERRANO, 2013) – serviram também para impulsionar críticas aos vieses de veículos midiáticos hegemônicos que criminalizavam esse tipo de protesto, caso específico do jornal *The New York Times*[7]. É nesse período também que se populariza o *distúrbio eletrônico*, famosa publicação do coletivo de artistas *Critical Art Ensemble* (CAE) que teoriza a desobediência civil eletrônica. Nas palavras de Milan (2013):

> O distúrbio eletrônico não foi um movimento de massa, mas sim um meio de intervenção baseado em células e caracterizado por ações bate-e-corre, as quais tiravam vantagem da descentralização típica da sociedade da informação. Em 1996, o grupo baseado no Texas conhecido como *Cult of the Dead Cow* cunhou o termo hackerativismo para descrever o vasto conjunto de atividades que se enquadram tanto em ativismo quanto em hackeamento, de forma a indicar o uso de expertise técnica como a programação motivada politicamente (MILAN, 2013, p. 5, tradução nossa).

Similarmente a essa percepção, Samuel (2004) caracteriza o ativismo hacker ou o hacktivismo como a união entre o ativismo político e o *hacking* de computador, através do uso não violento e legalmente ambíguo de ferramentas digitais com finalidades políticas. Tais ações são classificadas como atos de desobediência civil eletrônica justamente quando se valem do uso transgressivo de ferramentas digitais, tais como: desfiguração de sites (*Deface*); redirecionamento de páginas; negação de serviços (DDoS); apropriação de informações sigilosas (*Leak*); paródia de sites; manifestações e sabotagens virtuais; e desenvolvimento de softwares. É nesse sentido que essas atividades se diferenciam tanto das ações ciberativistas usuais (petições online, campanhas virtuais, fóruns de discussão, etc.), as quais se encontram nos limites convencionalmente aceitos da atuação política, quanto das atividades ciberterroristas, que fazem o uso da violência física ou psicológica para atingir objetivos próprios.

Dessa maneira, os hackers ativistas adotam causas políticas para justificar suas atividades, sendo "[...] o hacktivismo uma ação online politicamente motivada, ou uma campanha de

[7] O jornal publicou, em 4 de junho de 2000, a notícia "Police Brace For Protests In Windsor And Detroit", afirmando que os ativistas contrários à reunião da OMC atiraram pedras, coquetéis molotov e excrementos em policiais (Disponível em: <http://www.nytimes.com/2000/06/04/us/police-brace-for-protests-in-windsor-and-detroit.html>. Acesso em 25 abr. 2014). Embora o jornal tenha admitido posteriormente que o fato não era verídico, o artigo foi reproduzido por outros veículos midiáticos de grande repercussão. A correção da informação também foi ratificada, em 14 de setembro de 2000, pela própria Câmara da cidade de Seattle através do "Report of The WTO Accountability Review Committee Seattle City Council" (Disponível em: <http://www.seattle.gov/archive/wtocommittee/arcfinal.pdf>. Acesso em 25 abr 2014).

ações, realizada(s) por atores não-estatais em retaliação para expressar desaprovação ou para chamar a atenção a uma questão defendida pelos ativistas" (VEGH, 2003, p. 167, tradução nossa).

Mas, para que tais ações sejam consideradas como atos de desobediência civil eletrônica, Marion e Goodrum (2000), bem como Machado (2013), propõem certos requisitos, a saber: 1- não causem dano a pessoas ou a propriedades; 2- não sejam violentas; 3- não sejam desempenhadas visando ao lucro pessoal; 4- tenham motivações éticas, baseando-se na convicção de que a lei, norma ou conduta contra a qual se protesta é injusta; e 5- tenham, por parte de quem exerce essas ações, uma vontade de assumir as responsabilidades pessoais para as eventuais consequências.

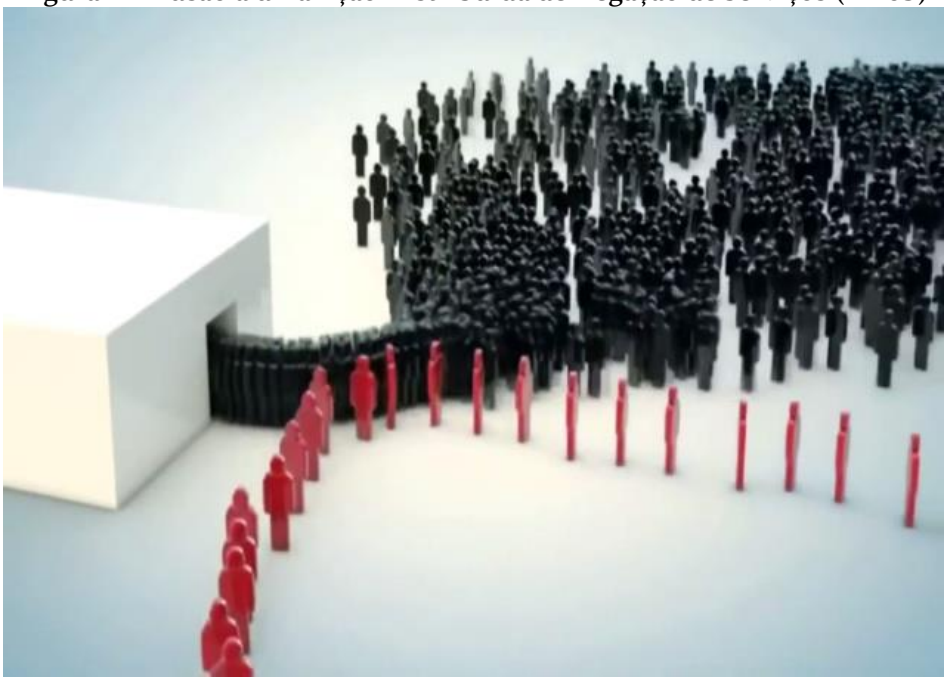
No entanto, após o atentado de 11 de setembro de 2001, quando ocorreram os ataques às Torres Gêmeas nos Estados Unidos, os discursos sobre os hackers na grande mídia passam a retratá-los não só como cibercriminosos comuns (visão popularmente atrelada a esses indivíduos), mas também como ciberterroristas. Desse modo, a criminalização do ativismo hacker e o combate ao anonimato na navegação em rede foram intensificados (VEGH, 2003). Isso se tornou bastante evidente quando da aprovação do Ato Patriota Norte-americano[8], nesse mesmo ano, o qual ampliou os mecanismos de vigilância do Governo (muitas vezes sem respaldo legal ou suspeitas fundamentadas) em nome da "guerra contra o terror". Essa coibição se mantém, como se pode comprovar , mais recentemente, na resposta do Presidente Barack Obama às denúncias de Edward Snowden[9]: "Você não pode ter 100% de segurança e ter também 100% de privacidade e 0% de inconveniência"[10]. De acordo com Assange et al. (2012), essa perspectiva se legitima sobretudo por meio da ideia de que há quatro cavaleiros do apocalipse da informação: pornografia infantil, terrorismo, lavagem de dinheiro e guerra contra as drogas, de modo que, sob o argumento de garantir a maior segurança da população, acaba-se legitimando a ampliação dos mecanismos de vigilância e transformando, portanto, todos os indivíduos em criminosos potenciais.

Ainda assim, o ativismo hacker ganha destaque no cenário político mundial em 2010 graças à atuação da rede hacktivista *Anonymous.* O gatilho para a popularização desse fenômeno foi o ciberataque conhecido como *#OpPayBack* que culminou na derrubada dos sites do *Paypal*, do *Mastercard* e da *Visa*, instituições financeiras responsáveis pelo bloqueio de donativos direcionados ao *WikiLeaks*[11]. Desde então, as ações de *DDoS* se tornaram uma das táticas mais recorrentes dessa rede como forma de protesto (COLEMAN, 2012; OLSON, 2014). Segundo Coleman (2012), as atividades dos *Anonymous* são mal definidas no plano legal e moral, pois ora se configuram como atos pacíficos e lícitos, ora são considerados como perturbadores e ilícitos. As ações de DDoS, por exemplo, simulam, no ambiente virtual, um protesto equivalente

[8] Lei nº 107-56/2001. Disponível em: <http://www.fincen.gov/statutes_regs/patriot/>.
[9] Ex-técnico da Agência de Segurança Nacional (NSA) que revelou alguns dos programas de vigilância dos Estados Unidos operados a partir da utilização de servidores de empresas como o *Google* e o *Facebook*.
[10] Matéria disponível em: <http://oglobo.globo.com/mundo/obama-ninguem-esta-escutando-as-suas-conversas-telefonicas-8617403>.
[11] Organização dedicada à publicação de documentos secretos que denunciam a conduta indevida de governos, empresas e instituições. O *WikiLeaks* se destacou em 2010 devido ao vazamento em massa de mais de 75 mil diários militares sobre a guerra do Afeganistão e de 251.287 comunicados diplomáticos de 274 embaixadas dos EUA (ASSANGE et al., 2012).

aos que costumam ocorrer no espaço físico, pois sobrecarrega o servidor de um site, impedindo as pessoas de utilizarem seus serviços. A figura 1 ilustra essa correspondência:

Figura 1 – Alusão a uma Ação Distribuída de Negação de Serviços (*DDoS*)



Fonte: Documentário *We are Anonymous – The Story of The Hacktivists*

Para Wong e Brown (2013), os *Anonymous* e o *WikiLeaks* são ativados pelo potencial de utilização do anonimato na internet e afetam as formas contemporâneas de se pensar o ativismo global ao se engajarem no que os autores nomeiam de "a política de ninguém". Isto é, as tecnologias informacionais não são apenas um meio para tomada de decisões políticas, pois redefinem também o próprio modo como a política se expressa:

> O potencial de anonimato da internet permite a emergência de diferentes tipos de protestos sociais. Ao contrário dos protestos físicos como uma demonstração de força, ativistas podem se reunir online, às vezes deliberadamente, às vezes acidentalmente, e expressar suas preferências políticas através do vazamento de informações ou atacando servidores (WONG; BROWN, 2013, p. 1024, tradução nossa).

Assim, através de protestos virtuais, fazem-se exigências sem a revelação dos indivíduos que estão por detrás delas (o *quem* importa menos do que o *como*). Além disso, se impõem custos materiais (sem deixar vestígios no espaço físico) quando, por exemplo, documentos sigilosos de autoridades públicas são vazados.

Por serem consideradas ilegais, os hacktivistas buscam legitimar essas manifestações perante a sociedade, a exemplo de petição encaminhada ao governo norte-americano[12], em 2013, quando indivíduos da rede *Anonymous* solicitaram o reconhecimento das ações de *DDoS* como uma manifestação legal de protesto. A intenção de associar o *DDoS* a um tipo de protesto, desvinculando-o da ideia de *ataque*, também foi exaltada pelo integrante do movimento em defesa do software livre, Richard Stallman (2011), na força tarefa virtual conhecida por *Opera-*

[12] "Anonymous exigiram legalizar ataques DDoS", Rádio Voz da Rússia, 2013. Disponível em: <br.sputniknews.com/portuguese.ruvr.ru/2013_01_10/anonymous-exigiram-legalizar-ataques-DdoS>. Acesso em: 11 dez. 2014.

ção *Payback*: "[...] a comparação mais adequada seria com as multidões que foram, em dezembro de 2010, protestar diante das lojas da Topshop (cadeia de varejo de moda no Reino Unido). Aquelas pessoas não invadiram as lojas e nem subtraíram dali nenhuma mercadoria, mas certamente provocaram um grande inconveniente" (STALLMAN, 2011, não paginado). Similarmente, o texto intitulado *Direito à demonstração online*, compartilhado por hacktivistas *Anonymous* em uma de suas operações, a *#OpGreenRights*[13], afirma que:

> A suspensão temporária de um serviço do site ou a divulgação das suas bases de dados não é uma ação violenta e não produz dano irreparável. Por essa razão, *DDoS*, *deface* e qualquer outra técnica que representa uma dissidência online têm que ser considerados como legais. Ferramentas computacionais de dissidentes são como um *flashmob* virtual. A violação de bases de dados causa danos leves e temporários para os empregados da empresa violada, mas permite solucionar os problemas dos segredos industriais e estatais, dando acesso à informação a todos os seres humanos. Por essas razões, a violação de bases de dados não pode ser considerada uma ação violenta, já que ajuda no crescimento do conhecimento comum. Nós consideramos a violação de bases de dados como os bloqueios que barcos ambientais fazem aos barcos pesqueiros, que, embora possam trazer desconforto temporário, não são considerados ilegais (*Anonymous*, online, tradução nossa).

2 Ativismo hacker no Brasil

As primeiras atividades de *Anonymous* brasileiros emergem a partir da Operação *Paypack* (*#OpPayback*) nos EUA, quando as ações dos *Anonymous* repercutiram mundialmente. De acordo com Machado (2013), essa operação impulsionou os brasileiros a buscarem mais informações sobre formas de engajamento em atos de apoio aos *Anonymous* na internet. Ao analisar duas operações capitaneadas em 2012 no Brasil – a Operacão *WeeksPayment* (*#OpWeeksPayment*) e a Operação Globo (#OpGlobo) –, o autor constata quatro modos de engajamento político dos *Anonymous* brasileiros, a saber: 1- promoção do anonimato, no qual a invisibilidade individual potencializa a visibilidade coletiva e serve como uma ferramenta política para os que não estão no poder; 2- a evangelização, realizada por colaboradores identificados com a ideia *Anonymous* através de postagens de informações sobre esse grupo em blogs, sites, redes sociais, etc.; 3- a formação de redes distribuídas, que consiste na formação de várias redes independentes entre si – em razão de haver vários indivíduos e métodos envolvidos – afim de dispersar o poder, tornando difícil o controle das atividades por parte de agentes externos; e 4- disseminação e viabilização de várias formas de ações políticas, já que se trata de um coletivo desprovido de lideranças centrais e da existência de um núcleo geográfico. Como prescindem da necessidade de vínculos formais (vínculos frágeis e temporários são mais típicos), os *Anonymous* facultam o surgimento de várias táticas possivelmente desconexas entre si, de acordo com os objetivos ideológicos de quem as executa.

3 Ativismo hacker e a legislação no Brasil

No direito brasileiro, o ativismo hacker gera implicações em três áreas: constitucional, penal e civil.

[13] Disponível em: <http://pastebin.com/LJpnSub6>. Acesso em: 11 dez. 2014

A Constituição assegura a liberdade de expressão em seu art. 5º, parágrafo IV; contudo, veda o anonimato, pois as pessoas têm que se responsabilizar por suas ações (BRASIL, 1988). À luz da interpretação literal, portanto, todos os indivíduos que se valem de algum artifício para ocultação de sua identidade civil praticam ato ilícito. Nas palavras do Ministro Celso de Mello, do Supremo Tribunal Federal (STF),

> O veto constitucional ao anonimato, como se sabe, busca impedir a consumação de abusos no exercício da liberdade de manifestação do pensamento, pois, ao exigir-se a identificação de quem se vale dessa extraordinária prerrogativa político-jurídica, essencial à própria configuração do Estado democrático de direito, visa-se, em última análise, a possibilitar que eventuais excessos, derivados da prática do direito à livre expressão, sejam tornados passíveis de responsabilização, "a posteriori", tanto na esfera civil, quanto no âmbito penal (BRASIL, 2002, não paginado).

Nessa perspectiva, a responsabilidade inerente à liberdade de expressão pode ser cível e/ou criminal.

A responsabilidade civil reside no dever de indenizar as pessoas ofendidas e que tenham sofrido danos morais e/ou materiais. Já a responsabilidade criminal engloba três crimes: injúria, calúnia e difamação.

Ocorre injúria quando se ofende a honra ou o decoro do indivíduo (Art. 140 do Código Penal). Calúnia acontece quando se imputa um fato criminoso a um indivíduo que não o praticou (Art. 138 do Código Penal); se o acusado praticou, não há crime, pois se trata de falar a verdade (exceção da verdade). Já a difamação ocorre quando se imputa a prática de um ato desonroso e não criminoso ao indivíduo que não o cometeu de fato (Art. 139 do Código Penal), ressalvada a exceção da verdade.

O Código Penal brasileiro, alterado pela Lei 12.737/12 (BRASIL, 2012), popularmente conhecida como "Lei Carolina Dieckmann", traz a tipificação penal para os crimes cibernéticos.

É fato que a Lei 12.737/12 veio atualizar o direito brasileiro, mas essa atualização legislativa é tardia e um tanto quanto simplista, o que pode dificultar a tipificação penal na prática, uma vez que o direito penal brasileiro é regido pelo princípio da estrita legalidade: *nullum crimen nulla poena sine lege praevia* ("não há crime tampouco punição sem a existência de lei criminal anterior ao ato" – art. 1º do Código Penal).

O simplista art. 154-A do Código Penal prescreve a conduta proibitiva de invadir dispositivo informático alheio com o objetivo de adulterar ou destruir dados e informações sem autorização do proprietário. O dispositivo prevê, ainda, a instalação de programas maliciosos para obtenção pessoal de vantagem ilícita como ato criminal, a exemplo de roubo de senhas de cartões de crédito ou acesso a redes sociais alheias. A punição para quem pratica esse crime é de detenção de três meses a um ano e multa.

É importante ressaltar que o código penal não prevê expressamente a hipótese de "violação" ao site, sobrecarga do sistema, que não é exatamente invasão de dispositivo informático.

No caso do ativismo hacker, a pena é ainda maior. Quando se tem acesso a informações privadas institucionais, segredos empresariais ou qualquer informação sigilosa oficial/estatal, a sanção passa a ser de reclusão, de seis meses a dois anos e multa (§3º, Art. 154-A). Em caso de divulgação das informações, que é comum nas táticas de *Leak* e *Exposed*[14], a punição é acrescida em dois terços (§4º, Art. 154-A).

O Código Penal assegura, ainda, uma maior punição quando esse tipo de ativismo é praticado contra Chefes do Executivo, Presidente do STF, Presidentes das Casas Legislativas ou dirigentes máximos da administração pública (§5º, Art. 154-A).

Com o intuito de abranger mais casos práticos, o Código Penal busca punir a interrupção, perturbação e atos que impeçam ou dificultem os serviços telemáticos ou de informação pública.

Em relação às alterações instituídas pela promulgação da Lei 12.737/12 no âmbito cível, temos a proteção constitucional à propriedade material e imaterial (Art. 5º) e a responsabilidade por danos materiais e morais. Ou seja, aquele que, por ação (dolo ou culpa) ou omissão, praticar ato que cause danos a outra pessoa comete ato ilícito e tem o dever de reparar os danos causados (Art. 186 do Código Civil).

O dano material corresponde ao efetivo prejuízo causado. Esse dano pode ser quantificado e, portanto, ressarcido. Já o dano moral é o sofrimento causado à vítima, o que não pode ser quantificado; é o constrangimento, exposição, humilhação, etc. Nesse caso, o dano moral não pode ser ressarcido, logo a indenização por danos morais tem a função de confortar a vítima para que possa suportar de forma mais digna os sofrimentos causados pelo agente.

Ainda no âmbito civil, temos o Marco Civil da Internet (MCR), Lei 12.965/14 (BRASIL, 2014), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O Art. 3º da Lei 12.965 assegura a liberdade de expressão, comunicação e manifestação do pensamento, sendo vedado, implicitamente, o anonimato constitucional. Para os hackerativistas, assim como para qualquer civil, vale esse mesmo fundamento jurídico no qual o MCR assegura o acesso à informação, ao conhecimento e à participação na vida cultural e na condução de assuntos públicos.

No entanto, há um impasse, pois informações obtidas pelos ativistas hackers por meio do uso ferramentas digitais transgressivas a respeito de assuntos públicos (como, por exemplo, esquemas de corrupção política ou obtenção de informações pessoais por empresas sem autorização do usuário) não podem ser usadas em eventuais processos penais no Brasil, pois as provas obtidas de forma ilícita não são admitidas (Art. 157, Código de Processo Penal).

[14]O *Leak* é o vazamento de informações de banco de dados de qualquer tipo. Um exemplo famoso de *Leak* é o já mencionado *WikiLeaks*, organização dedicada à publicação de documentos secretos que denunciam a conduta indevida de governos, empresas e instituições. O *Dox/Exposed* é a divulgação de informações particulares sobre alguma autoridade pública como forma de protesto. Um exemplo recente de *Dox* foi o vazamento de informações particulares do Presidente da Anatel em protesto à tentativa de limitação da internet.

4 Conclusões

Este trabalho apresentou as diferentes características do *hacking* político, confrontando duas abordagens que apontam para a legalidade ou não dos métodos disruptivos utilizados por hackers nessas ações. No Brasil, a vertente mais famosa do ativismo hacker é a rede *Anonymous*.

O ativismo hacker ou o hacktivismo é definido como a união entre o ativismo político e o *hacking* de computador através do uso não violento e legalmente ambíguo de ferramentas digitais com finalidades políticas. Tais ações são classificadas como atos de desobediência civil eletrônica justamente porque se valem do uso dessas ferramentas digitais de forma transgressiva, tais como: desfiguração de sites (*Deface*); redirecionamento de páginas; negação de serviços (*DDoS*); apropriação de informações sigilosas (*Leak*); paródia de sites; manifestações e sabotagens virtuais; e desenvolvimento de softwares.

No que concerne à legalidade das ações hacktivistas com fins de protesto, determinadas táticas são enquadradas juridicamente como criminosas. Tal visão legalista se contrapõe à perspectiva que coloca o ativismo hacker como um tipo de desobediência civil eletrônica, desde que haja propósitos bem delimitados e que sejam socialmente justificáveis.

É devido a essa ambivalência que ainda há controvérsias. A própria legislação ainda não é clara no tocante a esse tema. O *DDoS*, por exemplo, dependendo do modo como é executado, não configura uma invasão (conforme é previsto pela lei na qualidade de crime), mas sim uma sobrecarga no servidor em que determinado site está hospedado devido à enorme quantidade de requisições realizadas a ele.

Dada a complexidade de como essas ações são empreendidas, bem como das diferentes visões que a opinião pública tem a respeito dessas atividades, depreende-se que há uma linha bastante tênue, acerca desse tema, entre o que é permissível como uma forma legítima de protesto e o que pode ser considerado assertivamente como um cibercrime.

Parece que, tanto nas ciências sociais quanto no âmbito jurídico, o debate acerca dos protestos ocorridos no meio digital é ainda limitado e bastante vago, uma vez que, por se tratar de uma prática recente de engajamento político, não há uma compreensão mais ampla e crítica.

Espera-se, portanto, através deste estudo, ter contribuído para expandir e aprimorar o entendimento sobre o ativismo hacker, bem como para impulsionar a realização de futuros trabalhos a respeito dessa temática.

Referências

ASSANGE, Julian et al. **Cypherpunks**: a liberdade e o futuro da internet. São Paulo: Boitempo, 2012.

BRASIL. **Constituição [da] República Federativa do Brasil de 1988**. Brasília (DF), 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 27 abr. 2016.

BRASIL. Lei nº 12737, de 30 de novembro de 2012. **Lei 12.737/12**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 27 abr. 2016.

BRASIL.. Lei nº 12965, de 23 deabril de 2014. **Marco Civil da Internet**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 abr. 2016.

BRASIL. Supremo Tribunal Federal, Informativo STF, n. 286, 2002. Disponível em: <http://www.stf.jus.br/arquivo/informativo/documento/informativo286.htm>. Acesso em: 13 mar. 2015.

CLEAVER, Harry. Zapatistas e a teia eletrônica de luta. **Lugar comum**, v. 4, p. 139-163, 1998.

COLEMAN, Gabriela. Nossa esquisitice é livre. In: SILVEIRA, Sergio Amadeu da; JOSGRILBERG, Fabio B. (Orgs.). **Tensões em rede**: os limites e possibilidades da cidadania na Internet. São Paulo: Metodista, 2012.

MACHADO, Murilo Bansi. **Anonymous Brasil**: poder e resistência na sociedade de controle. Bahia: EDUFBA, 2013.

MARION, Mark; GOODRUM, Abby. Terrorism or civil disobedience: toward a hacktivistic ethic. **Computers and society**, v. 30, n. 2, p. 14-19, jul. 2000.

MILAN, Stefania. The guardians of the internet? Politics and ethics of cyberactivists (and of their observers). **Methodological and conceptual issues in cyber activism research**, National University of Singapore, 2013, p. 1-16. Disponível em: <https://citizenlab.org/wp-content/uploads/2012/08/NUS_Session-6_Stefania-Milan.pdf>. Acesso em 02 set. 2014.

MORAES, Denis de; RAMONET, Ignacio; SERRANO, Pascual. **Mídia, poder e contrapoder**: da concentração monopólica a democratização da informação. São Paulo: Boitempo, 2013.

OLSON, Parmy. **Nós somos Anonymous**: por dentro do mundo dos hackers. São Paulo: Novo Século, 2014.

SAMUEL, Alexandra Whitney. **Hacktivism and the future of political particiption**. 2004. 273 f. Tese (Doutorado em Ciência Política)–Departamento de Governo, Universidade Harvard, Cambridge/Massachusetts, 2004

SILVEIRA, Sérgio Amadeu da. Redes cibernéticas e tecnologias do anonimato. **Comunicação & Sociedade**, ano 30, n. 51, p. 113-134, 2009.

STALLMAN, Richard. "Ataque não, protesto!". **O Estado de São Paulo**, São Paulo, 3 jul. 2011. Redação Link. Disponível em: <http://blogs.estadao.com.br/link/ataque-nao-protesto/>. Acesso em: 11 dez. 2014.

VEGH, Sandor. **Hacking for democracy**: a study of the internet as a political force and its representation in the mainstream media. 2003. 349 f. Tese (Doutorado em Estudos Americanos)–Departamento de Estudos Americanos, Universidade de Maryland.

WONG, H. Wend; BROWN, Peter A. E-bandits in global activism: WikiLeaks, Anonymous, and the politics of no one. **Perspectives on politics**, v. 11, p. 1015-1033, 2013.

Bárbara Maria Farias Mota trabalhou na concepção, planejamento, análise, redação e revisão crítica do artigo.
Mestranda em Sociologia e Bacharela em Ciências Sociais pela Universidade Federal de Pernambuco (UFPE, Recife, Brasil). Integrante do Grupo de Métodos de Pesquisa em Ciência Política (DCP/UFPE, Recife, Brasil).
Renato Hayashi trabalhou na concepção da seção jurídica, redação e revisão crítica do artigo.
Advogado e Assessor Jurídico da Câmara Municipal do Recife (Recife, Pernambuco, Brasil). Mestrando em Políticas Públicas pela Universidade Federal de Pernambuco (UFPE, Recife, Brasil). Integrante do Grupo de Métodos de Pesquisa em Ciência Política (DCP/UFPE, Recife, Brasil). Especialista em Direito e Processo do Trabalho. Professor e coordenador de pós-graduação da Uninassau e da Faculdade Joaquim Nabuco.
Antônio Alves Tôrres Fernandes trabalhou na conclusão do artigo e na revisão substancial do texto.
Graduando em Ciência Política pela Universidade Federal de Pernambuco (UFPE, Recife, Brasil). Integrante do Grupo de Métodos de Pesquisa em Ciência Política (DCP/UFPE, Recife, Brasil). Bolsista da Fundação de Amparo à Ciência e Tecnologia de Pernambuco (FACEPE, Recife, Brasil).