Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral

Privacy as a threat to public security: A story of moral entrepreneurship

Arthur Coelho Bezerra *

RESUMO

O artigo trata da relação entre privacidade e segurança pública, tendo como base o discurso de autoridades norte-americanas (como o presidente Barack Obama e seu diretor de inteligência nacional) e brasileiras (como os deputados que assinam a recém-aprovada CPI dos Crimes Cibernéticos) sobre a importância do monitoramento e do acesso a dados pessoais como forma de combate a uma série de atividades criminosas. A hipótese é a de que a privacidade como "ameaça" é resultado de uma "cruzada moral" (nos termos de Howard S. Becker) que mascara as perspectivas de controle político e obtenção de vantagens econômicas oriundas das práticas de vigilância de comunicações digitais.

Palavras-chave: Privacidade; Segurança Pública; Vigilância; Empreendedorismo Moral; Crimes Cibernéticos.

ABSTRACT

The article deals with the relationship between privacy and public security, based on the speech by US (such as President Barack Obama and his Director of National Intelligence) and Brazil authorities (such as the deputies who signed the recently approved Cybercrime Report) on the importance of monitoring and access to personal data in order to combat a range of criminal activities. The hypothesis is that privacy as a "threat" is the result of a "moral crusade" (in terms of Howard S. Becker) that masks the prospects for political control and economic advantages derived from digital communication surveillance practices.

Keywords: Privacy; Public Security; Surveillance; Moral Entrepeneurship; Cibercrimes.

> *You can't have 100% security and also then have 100% privacy and zero inconvenience.*
>
> Barack Obama

INTRODUÇÃO

A relação entre privacidade e segurança pública é um dos principais temas de pesquisa no campo dos estudos sobre vigilância. Desde as reflexões de Michel Foucault (2012) sobre o panóptico de Jeremy Bentham, há cerca de 40 anos, a análise do uso de dispositivos de visibilidade para fins de controle social vem conquistando

* Doutor em Sociologia pela Universidade Federal do Rio de Janeiro. Pesquisador adjunto do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict). Professor do Programa de Pós-Graduação em Ciência da Informação (PPGCI-Ibict/UFRJ). Pesquisador do Núcleo de Estudos da Cidadania, Conflito e Violência Urbana (NECVU-UFRJ). Endereço: Rua Lauro Muller, 450, 4° andar, Botafogo, CEP 22290-160, Rio de Janeiro, RJ. Telefone: (21) 3873-9457. E-mail: arthurbezerra@ibict.br.

espaço na literatura científica de áreas como direito, ciências sociais, comunicação e, mais recentemente, ciência da informação. Tais estudos ganharam fôlego extra neste século, a partir da utilização de tecnologias digitais para a realização de monitoramentos massivos de dados e metadados, especialmente impulsionados pelos ataques ao World Trade Center em setembro de 2001 e amplamente discutidos após as denúncias de Edward Snowden, em 2013, sobre as práticas de vigilância mundial da agência de segurança norte-americana NSA.

David Lyon, diretor do Surveillance Studies Centre e editor da revista *Surveillance & Society*, afirma que, desde o 11 de setembro, diferentes formatos de vigilância, especialmente nos Estados Unidos, têm sido aceitos pela população sem resistência: "É possível que, de uma forma geral, cidadãos aceitem que a perda da privacidade seja o preço a ser pago pela segurança" (LYON, 2010, p. 116). A hipótese do sociólogo é a de que a cultura da TV e do cinema é uma das principais encorajadoras do perfil da "sociedade espectadora" que a todos observa (LYON, 2010, p. 117).

A esse respeito, podemos destacar também a cultura do medo, espetacularizada pelos mesmos canais de mídia que, muitas vezes, revelam-se mais decisivos para a orientação de políticas de segurança pública do que pesquisas científicas e estatísticas (CARDOSO, 2015). A explosão das torres gêmeas foi noticiada destacando a insegurança trazida pelas ameaças do "terrorismo", e o resultado político imediato seu deu na sanção, assinada pelo presidente George W. Bush apenas um mês e meio após os ataques, do USA Patriot Act, acrônimo para *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (em português, "Unindo e fortalecendo a América através do uso de ferramentas necessárias para obstruir o terrorismo"). Desde então, uma quantidade incomensurável de dados e metadados de comunicações vem sendo monitorada por órgãos do governo dos Estados Unidos e de outros países. Segundo as denúncias de Edward Snowden, além dos dados telefônicos, o *software* de vigilância Prism, usado pela NSA, coleta dados de provedores *online* incluindo *e-mail*, serviços de *chat*, vídeos, fotos, dados armazenados, transferências de arquivos, videoconferências e *logins*, e tem na lista de empresas envolvidas gigantes da internet como Yahoo, Microsoft, Facebook, Google (incluindo o YouTube), AOL e Skype (GREENWALD, 2014). O barateamento da tecnologia de computação permite que, em vez das antigas formas de vigilância direcionada, a coleta de informações possa ser feita em massa, o que significa o armazenamento de todas as telecomunicações, todas as chamadas de voz, todo o tráfego de dados e todas as maneiras pelas quais se consomem serviços de mensagem de texto (ASSANGE et al., 2013, p. 56).

Quando as denúncias de Snowden chegaram aos jornais, foram cobradas explicações do presidente Barack Obama a respeito do uso de programas para monitorar a população. Destacamos o seguinte trecho da resposta oficial de Obama:

> Eu acho que é importante reconhecer que não se pode ter 100 por cento de segurança e também ter 100 por cento de privacidade e zero de inconveniência. Nós vamos ter que fazer algumas escolhas como uma sociedade. E o que eu posso dizer é que, na avaliação desses programas, eles fazem a diferença na nossa capacidade de antecipar e evitar possíveis atividades terroristas.[1]

[1] Disponível em: <https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president>. Acesso em 6 de junho de 2016

No mesmo diapasão, o então diretor de inteligência nacional dos EUA, James Clapper, emitiu um comunicado no qual defende que "[...] os dados coletados sob o programa estão entre as mais importantes e valiosas informações, e são usados para proteger a nação de uma grande variedade de ameaças".[2] A palavra "ameaça" também surge, no Brasil, no recém-publicado relatório final da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos – que, no texto, são também chamados de "ameaças cibernéticas" (BRASIL, 2016, p. 88, 160, 176). Como exemplos, o relatório apresenta os conceitos de *worm, malware, spyware, botnet, backdoor, hoax, deface, keylogger, sniffer* e *phishing*.[3] Em resposta a tais "ameaças", o documento apresenta oito propostas de lei que, conforme se verá adiante, envolvem a diminuição dos direitos de privacidade dos usuários das redes digitais, alterando o panorama de proteção de dados garantido pela legislação brasileira desde a aprovação do Marco Civil da Internet em 2014.

Sob a ótica do presidente dos Estados Unidos, de seu diretor de inteligência e dos deputados que assinaram a mencionada CPI no Brasil, seria a própria privacidade uma das principais "ameaças" à segurança pública? É esta a indagação que irá nortear as próximas páginas deste artigo. A hipótese que apresentamos é a de que a privacidade como "ameaça" é, na verdade, resultado de uma "cruzada moral" (BECKER, 2008) que, embora ostente a garantia de melhorias na segurança pública como principal fator de legitimação, mascara as perspectivas de controle político e obtenção de vantagens econômicas oriundas das práticas de vigilância e monitoramento de comunicações digitais.

SOBRE O EMPREENDEDORISMO MORAL

O conceito de empreendedorismo moral foi cunhado por Howard S. Becker e apresentado em sua clássica obra *Outsiders* (publicada originalmente em 1963), tornando-se uma das principais contribuições do autor para os estudos da sociologia do desvio. De forma original, Becker defende que, ao estudarmos um determinado comportamento desviante, não devemos limitar nossa análise aos grupos que perpetram tal comportamento; devemos investigar, também, quem são os responsáveis por fazer com que aquele determinado comportamento seja socialmente reprovável, uma vez que é o estabelecimento de regras de conduta que qualifica certos comportamentos como desviantes, fazendo com que seus praticantes passem a ser vistos como *outsiders*.

> Regras sociais definem situações e tipos de comportamento a elas apropriadas, especificando algumas ações como "certas" e proibindo outras como "erradas". Quando uma regra é imposta, a pessoa que presumivelmente a infringiu pode ser vista como um tipo especial, alguém de quem não se espera viver de acordo com as regras estipuladas pelo grupo. Essa pessoa é encarada com um *outsider* (BECKER, 2008, p. 15).

---

[2] Disponível em: <http://ultimosegundo.ig.com.br/mundo/nyt/2013-06-07/eua-coletam-secretamente-dados-de-nove-empresas-de-internet.html>. Acesso em: 6 jun. 2016

[3] Em "Internet: uma sociologia de suas ameaças", tese de doutorado de Rodrigo Marques (2013), a lista é ainda mais extensa: a partir de um universo empírico composto por notícias e artigos publicados na imprensa brasileira, Marques estabelece uma tipologia das "ameaças" presentes no que chamou de "lado sombrio" da internet, catalogando 27 "males" que são analisados pelo autor à luz dos conceitos de "pânico moral", "risco" e "medo", conforme trabalhados pela literatura sociológica.

Assim como as regras que são forjadas no seio da sociedade, Becker entende que o desvio, no sentido de "erro publicamente rotulado", é também o resultado de um empreendimento moral. Antes que se qualifique um ato como desviante, alguém deve chamar a atenção pública para o assunto, conseguir transformar uma condenação moral em uma regra, e então na forma de lei, de modo a ser imposta para que se busque a não realização do ato que se julgava moralmente condenável. Sem esse empreendimento, "[...] o desvio que consiste na infração da regra não poderia existir" (BECKER, 2008, p. 167). Por isso, o autor conclama os sociólogos a incluir um conjunto mais amplo de pessoas e eventos em seus estudos dos fenômenos desviantes, levando em conta todos os participantes desses dramas morais, ou seja, tanto acusadores quanto acusados (BECKER, 2008, p. 206).

> Ao fazer de empreendedores morais (bem como daqueles a quem eles procuram controlar) objetos de estudo, essas análises violam a hierarquia de credibilidade da sociedade. Elas questionam o monopólio da verdade e "toda a história" sustentada pelos que ocupam posições de poder e autoridade. Sugerem que precisamos descobrir por nós mesmos a verdade sobre fenômenos supostamente desviantes, em vez de confiar em relatos oficiais certificados que deveriam ser suficientes para qualquer bom cidadão (BECKER, 2008, p. 207).

Se desejarmos aplicar o esforço sociológico sugerido por Becker a nosso objeto de pesquisa, devemos contemplar em nossa análise os grupos que promovem ações que restringem a proteção de dados pessoais nas redes digitais, afetando diretamente as perspectivas de privacidade dos usuários da internet como um todo. Para tanto, tomando como estudo de caso a CPI dos Crimes Cibernéticos, procuraremos, na próxima seção, compreender as razões que envernizam a legitimidade da cruzada moral perpetrada por tais agentes, uma vez que, além de justificar a existência de sua posição, os empreendedores morais devem ser capazes de impor não apenas regras, mas também o respeito da comunidade pelo trabalho que realizam (BECKER, 2008, p. 161-163).

A CRUZADA MORAL NA CPI DOS CIBERCRIMES

Em 31 de março de 2016, o Congresso brasileiro divulgou o relatório final da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, também conhecida como CPI dos Cibercrimes ou simplesmente CPI-Ciber. Conforme consta em sua própria folha de rosto, a CPI destinou-se a "investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a econômica e a sociedade neste país" (BRASIL, 2016, p. 1). O texto do relatório afirma que "o avanço tecnológico – sempre um passo à frente dos órgãos de repressão criminal – permitiu a atuação de delinquentes no ambiente virtual, cada vez mais protegidos pelo anonimato e impessoalidade que a internet permite" (BRASIL, 2016, p. 78).

Na seção intitulada "Justificativa", o relatório apresenta dados estatísticos que revelam os vultosos gastos com crimes cibernéticos no Brasil e apontam o incontestável aumento de diversas modalidades criminosas, como pornografia infantil ou pedofilia, racismo, homofobia, neonazismo, intolerância religiosa, maus-tratos contra os animais e incitação a crimes contra a vida, além de denúncias de vazamento de fotos íntimas, *hackeamento* de contas bancárias e de *e-mail*, fraudes e uma extensa lista de termos em inglês que se referem aos mais variados crimes cibernéticos. Na seção "Conclusões do relator", o deputado Espiridião Amin conta

que os deputados da comissão, "instruídos nas práticas nefastas de crimes digitais que ocorrem na grande rede", tiveram a oportunidade de verificar, por meio dos depoimentos e das investigações, "as agruras pelas que passam as vítimas e, também, as autoridades de investigação" (BRASIL, 2016, p. 170).

Em termos acadêmicos, os deputados procuram justificar a cruzada moral contra os crimes cibernéticos recorrendo, no relatório, ao artigo "Crimes cibernéticos: desafios da investigação", assinado pelo delegado de polícia e pesquisador de cibercrimes Silvio Castro Cerqueira e pelo consultor legislativo de segurança pública e defesa nacional Claudionor Rocha. Afirmam os autores:

> A instantaneidade das ações e a possibilidade de assincronia no uso da internet atenua os graus de segurança e certeza nas transações nela realizadas, o que gera a brecha (*breach*) para a atuação dos delinquentes. Cabe à norma de natureza penal, portanto, dispor a respeito dessas vulnerabilidades, de sorte a proteger os objetos jurídicos que o Estado considera sujeitos à tutela legal (CERQUEIRA; ROCHA, 2013, p. 139 apud BRASIL, 2016, p. 79).

Em outra passagem do artigo, os autores citam o projeto de lei 84/99, do senador Eduardo Azeredo, como um exemplo jurídico de "facilitação de investigação de crimes cibernéticos" (CERQUEIRA; ROCHA, 2013, p. 140). Tal "facilitação" advinha, sobretudo, da previsão de guarda, por parte das empresas de conexão à internet, de dados de usuários por três anos para fins de possível investigação criminal, além de multa e detenção por até dois anos para quem utilizasse senhas digitais de forma não autorizada. Esses pontos polêmicos fizeram emergir, em 2009, uma campanha de diversos setores da sociedade civil – como os participantes do Fórum Brasileiro Software Livre, professores da Escola de Direito da Fundação Getúlio Vargas e outros – que se manifestaram contra o projeto, chamado por seus opositores de "AI-5 Digital" (SOLAGNA; SOUZA; LEAL, 2015).

A reação à cruzada moral prevista pela Lei Azeredo resultou na paralização da tramitação do projeto de lei e levantou o debate sobre a necessidade de um marco regulatório para a internet brasileira. A partir desse debate, a Secretaria de Assuntos Legislativos do Ministério da Justiça estabeleceu uma parceria com a FGV-Rio para criação de uma plataforma digital, com vistas à construção colaborativa do que viria a se tornar o Marco Civil da Internet, sancionado pela Presidência em 2014.

Embora a análise das disposições do Marco Civil fuja ao escopo do presente artigo, é importante ressaltar o reconhecimento, por parte de Cerqueira e Rocha (2013, p. 137), de que "a nova lei trouxe garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações", bem como a "vedação de divulgação dos dados pessoais". A mesma frase é citada no relatório da CPI dos Cibercrimes, que acrescenta:

> [A lei do Marco Civil da Internet é] considerada uma das leis mais avançadas no tema. Por essa razão vários países têm se inspirado na norma brasileira para editar suas próprias leis sobre o assunto. Resultado de intensa discussão parlamentar, com a participação direta da sociedade por meios dos canais que a própria internet propiciou, o MCI buscou o justo equilíbrio entre os interesses em disputa, variando desde os extremos que propunham estrito controle ou liberdade total (BRASIL, 2016, p. 79)

No entanto, após apresentar uma série de estatísticas que apontam o aumento de crimes cometidos pelas redes digitais e de catalogar as mais variadas ameaças às quais o usuário da internet pode estar exposto, o relatório propõe oito projetos de lei que incluem alterações na legislação do Marco Civil da Internet, não obstante considerada, como visto, "uma das leis mais avançadas sobre o tema".

Entre as alterações, está a proposta de incluir no rol das informações cadastrais de usuários o endereço dos computadores (o chamado *internet protocol* – IP) no momento de criação da conta de internet. Na prática, significaria que as autoridades policiais poderiam requisitar aos provedores de conexão o endereço IP de qualquer pessoa investigada, sem necessidade de autorização judicial. O relatório critica a atual demora da obtenção dessa informação, justamente por conta da exigência de mandato judicial que o Marco Civil prevê, e defende que a mudança na lei "permitiria a identificação de internautas investigados de maneira automática e imediata" (BRASIL, 2016, p. 205), complementando:

> Gostaríamos de ressaltar neste ponto do relatório que a equiparação que ora propomos não implica em franquear o acesso a policiais aos dados de qualquer internauta [...]. Apenas poderão ser obtidos dados pessoais de cadastro para fins de investigação, isto é, com processos investigatórios já abertos. Qualquer uso desses dados em desacordo com esse princípio continuará sendo considerado abuso de autoridade. Dessa maneira, os internautas que não tiverem cometido nenhum tipo de crime possuem a garantia de manutenção de sua intimidade (BRASIL, 2016, p. 206)

Se por um lado, a retórica do texto reforça o bordão "se você não tem nada a esconder, não tem nada a temer", por outro legitima a presunção de culpa de toda pessoa investigada. Além disso, conforme aponta o documento do Instituto de Tecnologia e Sociedade sobre o relatório da CPI-Ciber, a medida alça delegados à condição de juízes, violando, inclusive, a recomendação do Relatório Especial da ONU para Liberdade de Expressão, que exige que qualquer determinação nesse sentido deva ser feita por uma autoridade judiciária competente.[4]

DIREITOS AUTORAIS: A CEREJA DO BOLO DA CRUZADA MORAL

O uso não autorizado de conteúdos protegidos por leis de direitos autorais, ato legalmente tipificado como pirataria no Brasil desde 2004, é uma prática trivial e recorrente nas redes digitais da internet. A grande maioria de vídeos, fotos e textos compartilhados no ambiente *online* é feita sem o consentimento dos detentores de seus direitos autorais, o que caracteriza um tipo de infração previsto em lei. Entretanto, o relatório final da CPI dos Cibercrimes dedica apenas 5 parágrafos de suas 254 páginas ao tema. A breve seção 2.1.4, intitulada "Violação de direitos autorais na internet", é iniciada com um parágrafo revelador:

> Quanto à violação de direitos autorais na internet, esta CPI não teve tempo hábil para se debruçar sobre a legislação específica do tema. Todavia, entendemos que a legislação vigente é insuficiente, uma vez que não prevê qualquer mecanismo efetivo que permita à autoridade judicial bloquear junto às operadoras o acesso a sítios

[4] Disponível em: <http://itsrio.org/projects/contribuicao-atualizado-ao-relatorio-da-cpi-ciber/>. Acesso em: 25 jun. 2016

> de internet que distribuam conteúdos protegidos distribuídos de maneira ilegal, os chamados "*sites* de conteúdos piratas" (BRASIL, 2016, p. 136).

A ignorância sobre o tema, reconhecida no próprio texto do relatório, não pareceu servir de constrangimento para a manifestação de "apoio à inclusão, pela Comissão Especial de Direito Autoral, de dispositivo que permita o bloqueio de sítios que veiculem conteúdos protegidos por direito autoral de maneira ilegal pelas operadoras de conexão à internet mediante ordem judicial" (BRASIL, 2016, p. 137). Com efeito, em uma nota de esclarecimento da CPI, divulgada um mês após a apresentação do relatório, os deputados propõem um novo texto para o projeto de lei do Bloqueio que deixa claro o nivelamento da violação de direitos autorais com crimes de mais grosso calibre:

> Nova redação ao "projeto de lei do bloqueio" (item 1.6), listando de maneira extensiva, quais são as condutas criminosas que poderão ensejar o bloqueio de sítios. A saber, apenas aquelas relacionadas a: i) terrorismo; ii) crimes hediondos (incluindo a venda de medicamentos que menciona); iii) tráfico de drogas; iv) pedofilia; v) tráfico internacional de armas; vi) violação de propriedade intelectual; vii) crimes contra a propriedade industrial; e viii) violação de direito de autor de programa de computador (grifo dos autores). [5]

A aproximação da violação de direitos autorais com práticas mais ofensivas não é um expediente novo. A cruzada moral contra a pirataria se vale de técnicas semelhantes: por um lado, os empreendedores morais da indústria cultural tratam a pirataria como um tipo de furto, como se baixar um arquivo ou comprar um produto pirata fosse o mesmo que subtrair um objeto de alguém; por outro lado, estimulam a associação entre a violação de direitos autorais e a violação de propriedade industrial (patentes de invenção, marca e *design*), de forma a incluir no rol da pirataria os crimes de falsificação e contrafação (BEZERRA, 2014). Foi esse o entendimento adotado pela Comissão Parlamentar de Inquérito que, apesar de se chamar CPI da Pirataria, investigou também a falsificação e o contrabando de brinquedos, bebidas, cigarros e outros produtos no Brasil em 2004. De acordo com o relatório final dessa CPI, "a pirataria abrange, na realidade, toda espécie de adulteração e falsificação de produtos, promovendo com isto incalculáveis prejuízos ao consumidor e estupendo desvio de impostos que poderiam ser revertidos em serviços públicos visando ao bem-estar da população brasileira" (apud BEZERRA, 2014, p. 131).

Com a CPI dos Cibercrimes, aprovada em 4 de maio de 2016 com a citada emenda no projeto de lei do Bloqueio, a cruzada moral contra a pirataria ganha novo impulso, e abre um perigoso precedente para a limitação do exercício de liberdade de expressão nas redes digitais, conforme se verá adiante.

---

[5] Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/outros-documentos/nota-de-esclarecimento-sub-relatores-deputados-sandro-alex-e-rafael-motta>. Acesso em: 13 jun. 2016.

CONTROLE POLÍTICO E VANTAGENS ECONÔMICAS: OS MOTIVOS NÃO DECLARADOS

Embora se possa ter uma ideia do empreendedor moral como alguém que simplesmente deseja impor seu interesse em detrimento dos demais, em muitos casos esse agente acredita que atua em nome de um bem maior, e que se as pessoas fizerem o que julga certo, será melhor para elas. Becker cita os exemplos históricos dos defensores da Lei Seca, com suas preocupações com a saúde das pessoas, e dos abolicionistas, preocupados com a vida da população negra, para explicar que o empreendedor moral pode realmente acreditar que sua reforma evitará certos tipos de exploração de uma pessoa por outra (BECKER, 2008, p. 153-154).

De fato, vimos que os deputados procuram demonstrar sua preocupação com "as agruras pelas que passam as vítimas e, também, as autoridades de investigação". Mencionamos a referência aos gastos com os crimes cibernéticos e seus devastadores prejuízos – o texto do relatório chega a citar o exemplo de uma invasão de *crackers* à plataforma da Sony, fabricante do videogame Playstation, que teria custado mais de 37 bilhões à empresa (BRASIL, 2016, p. 9).[6] É, sobretudo, contra a "prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país" que a CPI finca o alicerce que legitima sua própria existência.

Semelhantes são as falas de Barack Obama e de seu diretor de inteligência nacional, citadas na introdução deste artigo. A demonstração de preocupação com questões referentes à segurança pública e à defesa nacional é o que parece legitimar, em seus discursos, a impossibilidade de se ter "zero por cento de inconveniência". A tolerância à invasão de privacidade perpetrada pelas agências de segurança seria o preço a ser pago por cidadãos que desejam viver em uma sociedade de baixo risco.

Entretanto, embora a motivação alegada para todo o aparato de vigilância estadunidense gravite em torno do que Julian Assange e Jacob Applebaum chamaram de "os Quatro Cavaleiros do Infoapocalipse: lavagem de dinheiro, drogas, terrorismo e pornografia infantil" (ASSANGE et al., 2013, p. 87), as denúncias de Edward Snowden revelaram que a NSA também levantou dados sobre empresas de petróleo no Brasil e na Venezuela e de energia no México, além de ter mapeado a movimentação das Forças Revolucionárias da Colômbia (Farc) e de ter registrado conversas telefônicas da presidente do Brasil e da chanceler da Alemanha, entre outros líderes políticos. Ao citar o risco de uma empresa norte-americana de petróleo conseguir mapear a estratégia de investimentos da Petrobras ou dos benefícios que o setor agrícola dos Estados Unidos teria a partir do rastreamento de informações do agronegócio brasileiro, o jornalista Luciano Martins Costa afirma que, "se a espionagem americana no Irã e no Paquistão é motivada por questões de segurança, o monitoramento das comunicações na China e no Brasil deve ter outras razões, uma vez que esses dois países estão fora do mapa principal do terrorismo internacional" (apud BEZERRA; SCHNEIDER; SALDANHA, 2013, p. 12).

Coincidentemente, na mesma época em que as denúncias de Snowden chegavam à grande mídia, o número de protestos políticos no Brasil crescia vertiginosamente,

[6] Este cálculo superestimado parte da mesma lógica discutível que norteia as pesquisas encomendadas pelas indústrias de conteúdo (das quais a Sony faz parte) sobre os prejuízos causados pela pirataria, que atribuem uma "implausível relação de causalidade" entre o consumo de um conteúdo pirata e uma disposição do comprador em adquiri-lo, caso não tivesse acesso ao conteúdo gratuitamente (BEZERRA, 2014, p. 125). Em outras palavras, é implausível supor que a Sony teria faturado 37 bilhões caso os *crackers* não invadissem a plataforma do Playstation.

chegando a milhões de participantes. Em 23 de julho de 2013, na esteira das manifestações que, entre outras coisas, revelaram a grande impopularidade do governo do estado do Rio de Janeiro, foi publicado no *Diário Oficial* o decreto 44.302/2013, assinado pelo então governador Sérgio Cabral, criando a Comissão Especial de Investigação de Atos de Vandalismo em Manifestações Públicas (Ceiv). O texto de tal decreto diz que "caberá à Ceiv tomar todas as providências necessárias à realização da investigação da prática de atos de vandalismo, podendo requisitar informações, realizar diligências e praticar *quaisquer atos necessários* à instrução de procedimentos criminais com a finalidade de punição de atos ilícitos praticados no âmbito de manifestações públicas" (grifo nosso). Em outra passagem, é decretado que "as empresas operadoras de telefonia e provedores de internet terão prazo máximo de 24 horas para atendimento dos pedidos de informações da Ceiv".

Não precisamos entrar no mérito de questionar a inconstitucionalidade do decreto, uma vez que o mesmo sofreu críticas tanto por parte da população quanto de instituições como a Ordem dos Advogados do Brasil, sendo por fim suspenso. O que importa destacar são os potenciais efeitos devastadores sobre a privacidade de qualquer pessoa considerada suspeita por participar de um ato público contra o poder constituído. Nesse ponto, cabe indagar: é possível acreditar que se tratava apenas de uma cruzada moral contra "atos ilícitos"? A prisão, um dia antes da final da Copa do Mundo em 2014, de 23 manifestantes considerados perigosos por estarem envolvidos em atos violentos em manifestações nos leva a questionar a afirmação anterior. E o projeto de lei da CPI dos Cibercrimes, que inclui o endereço de IP como um dos dados obrigatórios a serem oferecidos às autoridades para fins de investigação, na prática, pode atuar como instrumento de desmobilização política ou de punição por oposição política, na medida em que permite a violação da privacidade a partir de suspeita (sempre subjetiva) de associação com atos de violação da ordem pública.

Com a cereja do bolo representada pela inclusão da violação dos direitos autorais no projeto de lei do Bloqueio, abre-se a oportunidade de benefícios econômicos para empresas e vantagens políticas para governantes. Na cruzada moral da indústria cultural contra a pirataria, vemos que, por trás dos declarados motivos de necessidade de retorno financeiro para que artistas tenham estímulos para a produção cultural, esconde-se a tentativa de manutenção do domínio de mercados econômicos, mediante o controle hegemônico dos fluxos de bens culturais. O caminho tomado pelos "empreendedores morais da cultura" foi definir a pirataria como o inimigo público número um e investir todas as forças em uma verdadeira guerra contra esse inimigo, incluindo estratégias jurídicas, campanhas publicitárias, ações em escolas e uma série de outras ofensivas (BEZERRA, 2014). A inclusão das violações de direitos autorais no mencionado projeto de lei da CPI dos Cibercrimes pode ser considerada uma vitória desses grupos.

Sem embargo, não é apenas a indústria cultural que angaria benefícios com o bloqueio de material considerado pirata. Em artigo publicado na página da Eletronic Frontier Foundation, uma das mais atuantes organizações de defesa de direitos civis no mundo digital, Maira Sutton demonstra preocupação com o abuso de notificações de violação de *copyright* para silenciar críticas políticas na internet. Entre os exemplos citados, a autora menciona a derrubada de vídeos críticos ao candidato derrotado à Presidência de 2014, Aécio Neves, que foram retirados do ar sob a justificativa de violação de direitos autorais (suspeita-se, a pedido do próprio Neves).

> Quando as autoridades estaduais procuram censurar o discurso *on-line*, eles vão usar o método mais rápido e mais fácil disponível.

> Para muitos, avisos de remoção de direitos autorais dão conta do recado. Depois de anos de *lobby* e pressão crescente de indústrias de conteúdos sobre os responsáveis políticos e as empresas de tecnologia, o envio de avisos de direitos autorais para tirar mídias do ar está mais fácil do que nunca (tradução nossa).[7]

Grande parte do conteúdo criativo disponível na internet é resultado de bricolagens, *remixes* e *mashups*: são criações a partir de algum conteúdo já existente, majoritariamente produzidas sem qualquer pedido de autorização. Imagens como memes e páginas como Tumblr são recursos amplamente utilizados para a criação cultural e a manifestação política, e não raro obedecem à lógica híbrida e antropofágica de produção artística das redes digitais. A possibilidade de um político exigir o bloqueio de um conteúdo que lhe seja crítico, tendo como justificativa o uso de uma foto sua que possui direitos autorais reservados, é um dos desdobramentos do citado projeto de lei da CPI dos Cibercrimes.

CONCLUSÃO

Durante a redação deste artigo, a população dos Estados Unidos sofreu a pior tragédia em seu território desde os atentados de 11 de setembro de 2001: o assassinato a sangue frio de mais de 50 pessoas em uma boate de Orlando voltada para o público LGBT. O assassino já havia sido interrogado duas vezes em 2013 pelo FBI por suspeitas de ligação com terroristas do Estado Islâmico; ainda assim, a maior potência do mundo, dotada do maior aparato de vigilância em massa da história, não foi capaz de prever e evitar a tragédia. Por outro lado, há reportagens publicadas na revista *Newsweek*,[8] no jornal *The Guardian*[9] e em outros canais de mídia que apontam que os ataques de 11 de setembro poderiam ter sido evitados pela simples adoção dos procedimentos de segurança vigentes à época.

Essas duas informações nos levam a refletir sobre a eficácia da política de vigilância massiva de dados pessoais e sobre a legitimidade do discurso que defende a diminuição das garantias de privacidade como forma de recrudescimento da segurança pública. A essa altura, cabe questionar: os programas de vigilância em massa realmente "fazem a diferença na nossa capacidade de antecipar e evitar possíveis atividades terroristas", como enfatizou o presidente Barack Obama no trecho destacado no início deste artigo?

Na mesma fala, Obama afirma que "nós vamos ter que fazer algumas escolhas como uma sociedade". Se está claro que a dimensão da privacidade, seja em seu foro íntimo ou em seu arcabouço jurídico, é uma escolha da sociedade, é importante que esta sociedade exerça tal escolha participando da arquitetura das leis que, em última instância, irão contribuir para a definição dos próprios contornos da privacidade e de sua forma social de manifestação. Nesse sentido, é oportuno resgatar o exemplo do Marco Civil da Internet, construído mediante uma inédita consulta pública *online*, que

---

[7] Disponível em: <https://www.eff.org/deeplinks/2014/12/copyright-law-tool-state-internet-censorship>. Acesso em: 13 jun. 2016

[8] Disponível em: <http://www.newsweek.com/2015/01/23/information-could-have-stopped-911-299148.html>. Acesso em: 15 jun. 2016

[9] Disponível em <https://www.theguardian.com/world/2004/mar/23/usa.september11>. Acesso em: 15 jun. 2016.

contou com centenas de contribuições de diferentes organizações e espaços institucionais.

> No contexto brasileiro, a incorporação de diferentes atores oriundos de movimentos tecnopolíticos na condução de políticas públicas na área de tecnologias de informação e comunicação (TICs), dentro do Estado, contribuiu para a construção de um amplo campo de *advocacy* em favor de uma legislação focada na garantia de direitos mínimos sobre a rede (SOLAGNA; SOUZA; LEAL, 2015, p. 129)

O Marco Civil foi aprovado em 2014, tornando-se o principal parâmetro legal para questões relacionadas à privacidade e à proteção de dados pessoais nas redes digitais. Também foi aprovado, em 4 de maio de 2016, o relatório final da CPI dos Cibercrimes, que, apesar de sofrer alterações em relação ao texto original, apresenta projetos de lei que alteram as disposições do Marco Civil no tocante à privacidade, o que vem gerando críticas por parte de setores que defendem a manutenção dos tais "direitos mínimos" adquiridos pela lei vigente.

Em paralelo, tramitam no Congresso Nacional três iniciativas que pretendem regulamentar de forma abrangente a proteção de dados pessoais no Brasil, sendo um projeto de lei oriundo da Câmara dos Deputados, um outro do Senado e um terceiro de autoria do Poder Executivo. Em um gradiente de visões que vão do reducionismo ao expansionismo, cada uma dessas leis possui seu conceito específico do que sejam dados pessoais, e "diferenças sutis em torno da sua definição implicam em consequências drásticas para o alcance dessa proteção".[10] A escolha entre uma dessas visões é de fundamental interesse da sociedade; à pesquisa científica, cabe não apenas angariar informações e produzir conhecimentos para auxiliar nessa importante tomada de decisão, mas também, no sentido de cumprir sua função social, destacar a importância da participação pública na esfera política.

Artigo recebido em 07/07/2016 e aprovado em 17/11/2016.

REFERÊNCIAS

ASSANGE, J. et al. *Cypherpunks*: liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

BECKER, H. S. *Outsiders*: estudos de sociologia do desvio. Rio de Janeiro: J. Zahar, 2008.

BEZERRA, A. *Cultura ilegal*: as fronteiras morais da pirataria. Rio de Janeiro: Mauad X: Faperj, 2014.

BEZERRA, A; SCHNEIDER, M.; SALDANHA, G. S.. Ascensão e queda da utopia tecnoliberal: a dialética da liberdade sociotécnica. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Florianópolis. *Anais eletrônicos...*

[10] A frase consta no relatório do Grupo de Pesquisa em Políticas Públicas para o Acesso a Informação da Universidade de São Paulo (GPoPAI/USP), que se debruçou sobre a forma como os conceitos e referenciais teóricos da proteção dos dados pessoais foram tratados nos três citados projetos de lei. Disponível em: <https://gpopai.usp.br/wordpress/wp-content/uploads/2016/06/Xeque-Mate.pdf>. Acesso em: 15 jun. 2016.

Rio de Janeiro: Ancib, 2013. Disponível em: <http://enancib.sites.ufsc.br/index.php/enancib2013/XIVenancib/paper/viewFile/364/358>. Acesso em: 25 jun. 2016.

BRASIL. Câmara dos Deputados. Comissão Parlamentar de Inquérito de Crimes Cibernéticos. *Relatório final.* Brasília, 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015>. Acesso em: 25 jun. 2016

CARDOSO, B. *Todos os olhos*: videovigilâncias, voyeurismos e (re)produção imagética. Rio de Janeiro: Ed. UFRJ: Faperj, 2015

CERQUEIRA, S. C.; ROCHA, C. Crimes cibernéticos: desafios da investigação. *Cadernos Aslegis,* Brasília, n. 49, p. 131-161, maio/ago. 2013.

FOUCAULT, M.. *Vigiar e punir*: nascimento da prisão. Petrópolis: Vozes, 2012.

GREENWALD, G. *Sem lugar para se esconder.* Rio de Janeiro: Sextante, 2014.

LYON, D. 11 de setembro, sinóptico e escopofilia: obervando e sendo observado. In: BRUNO, F.; KANASHIRO, M.; FIRMINO, R. (Org.). *Vigilância e visibilidade*: espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

MARQUES, R. *Internet*: uma sociologia de suas ameaças. Rio de Janeiro, 2013. Tese (Doutorado em Sociologia) – Instituto de Filosofia e Ciências Sociais, Universidade Federal do Rio de Janeiro.

SOLAGNA, F.; SOUZA, R. H. V.; LEAL, O. F. Quando o ciberespaço faz suas leis: o processo do Marco Civil da Internet no contexto de regulação e vigilância global. *Vivência*: revista de antropologia, Natal, v. 1, n. 45, p. 127-144, jan./jun. 2015. Dossiê Antropologia da Cibercultura.