Cadernos do Programa de Pós-Graduação DIREITO/UFRGS
volume11| n.1 | 2016 | seer.ufrgs.br/ppgdir

INTERNET E PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DAS NORMAS JURÍDICAS BRASILEIRAS A PARTIR DAS REPERCUSSÕES DO CASO NSA VS. EDWARD SNOWDEN

INTERNET AND PROTECTION OF PERSONAL DATA: AN ANALYSIS OF BRAZILIAN LEGAL STANDARDS THROUGH THE REPERCUSSIONS OF THE CASE NSA VS. EDWARD SNOWDEN

Salete Oro Boff[*]
Vinícius Borges Fortes[**]

RESUMO: A Constituição Federal do Brasil, no artigo 5º, inciso X, assegura a inviolabilidade da vida privada, da intimidade e da honra como um direito fundamental. O Marco Civil da Internet instituiu, no Brasil, diversidade de princípios e parâmetros para a regulação da internet no país. Observa-se, assim, a existência de uma lacuna no sistema jurídico brasileiro, de norma e infraestrutura, para a efetivação da garantia ao direito à proteção dos dados na internet como em outros países. Esta pesquisa busca responder em que medida a norma jurídica brasileira esta adequada como resposta aos atos de vigilância e monitoramento de informações e dados pessoais dos usuários praticada pela *NSA – National Security Agency*, a partir dos objetivos de (i) observar e mapear a interação de diálogos sociais e institucionais dos Estados Unidos na formação do *backlash* do caso *NSA vs. Edward Snowden*; (ii) observar e mapear os resultados da formação do *backlash* do caso *NSA vs. Edward Snowden* a partir do reconhecimento da violação do direito à privacidade e à proteção dos dados pessoais como violação de direitos humanos; (iii) observar e mapear as normas jurídicas brasileiras constituídas a partir da compreensão jurídica da internet e as repercussões do caso *NSA vs. Edward Snowden*. A pesquisa desenvolve o método de análise do mapeamento crítico, analisando comparativamente a interação de diálogos sociais e institucionais nos Estados Unidos na formação do *backlash* no caso *NSA vs. Edward Snowden*, relacionado à vigilância e monitoramento de dados e informações pessoais pela agência estadunidense. O mapeamento crítico proposto nessa pesquisa leva em consideração os marcos regulatórios para a governança da internet no Brasil, e que tenham por escopo assegurar a proteção jurídica do direito à privacidade, à inviolabilidade dos dados pessoais, em equilíbrio com o direito ao acesso à informação, sobretudo em relação ao tema do estudo, que se concentra na compreensão de que a violação do direito à privacidade e à proteção dos dados pessoais configura uma transgressão aos direitos humanos. A pesquisa identifica que o Brasil possui normas jurídicas que atendem parcialmente aos anseios da sociedade em relação à proteção de dados pessoais, especialmente após a repercussão dos atos de vigilância em massa promovidos pelo governo dos EUA.

ABSTRACT: *Brazilian Federal Constitution, Article 5, section X, ensure the inviolability of privacy, intimacy and honour as a fundamental right. The Brazilian Internet Bill of Rights (also called 'Marco Civil da Internet') instituted a diversity of principles and parameters for regulation of Internet in Brazil. Therefore, it can be verified the existence of a gap in Brazilian legal system, which cannot assure as effective guarantee to the right to data protection on the Internet as identified in other countries. This research seeks to analyze to what extent the Brazilian legal rules are appropriate to answer acts of surveillance and monitoring of information and personal data of users practiced by the NSA - National Security Agency. Its aim is (i) to observe and map the interaction between social and institutional dialogues in US in the backlash formation of the NSA vs. Edward Snowden case; (ii) to observe and map the results of the formation of the backlash of the NSA vs. Edward Snowden case through the recognition of the infringement of the right to privacy and protection of personal data as an infringement of human rights; and (iii) to examine and map Brazilian legal rules established based on a legal understanding of the Internet and the repercussions of the NSA vs. Edward Snowden. This research was developed through the method of analysis of critical mapping, comparatively analysing the interaction of social and institutional dialogue in the United States in the formation of backlash of NSA vs. Edward Snowden, which was related to the surveillance and the monitoring of data and personal information by the US agency. The critical mapping proposed in this study takes into account regulatory frameworks for the governance of the Internet in Brazil that have the scope to ensure legal protection of the right to privacy and inviolability of personal data, in balance with the right of access to information. The research emphasizes the understanding that the infringement of the right to privacy and the protection of personal data constitutes a violation of human rights. The study identifies that Brazil has legal rules that partially meet social concerns regarding the protection of personal data, especially after the impact of actions of mass surveillance promoted by the US government.*

[*] Pós-doutora pela Universidade Federal de Santa Catarina (UFSC). Doutora em Direito pela Universidade do Rio dos Sinos (UNISINOS). Professora do Programa de Pós-Graduação da Faculdade Meridional (IMED), Rio Grande do Sul.

[**] Doutor em Direito pela Universidade Estácio de Sá (UNESA), Rio de Janeiro, na linha de pesquisa Direitos Fundamentais e Novos Direitos. Professor do curso de Direita da Faculdade Meridional (IMED), Rio Grande do Sul.

Cadernos do Programa de Pós-Graduação DIREITO/UFRGS
volume11| n.1 | 2016 | seer.ufrgs.br/ppgdir

PALAVRAS-CHAVE: Privacidade. Vigilância em massa. Ciberespaço. *NSA vs. Edward Snowden*.

KEYWORDS: *Privacy. Surveillance. Cyberspace. Human rights. NSA vs. Edward Snowden.*

INTRODUÇÃO

O progresso da humanidade se reflete, também, na capacidade de transmitir informações e as questões de "tempo e distância" no campo da informação tem sua dimensão reduzida. Com isso, o direito à informação expandiu-se, facilitando o acesso ao conhecimento, nos mais diversos pontos do planeta. Esse espaço 'virtual' criado, ou ciberespaço, é um espaço social, formado pelo fluxo de informações e dados transmitidos entre computadores, constituindo-se como uma rede aberta na qual qualquer pessoa pode ter acesso com a possibilidade de interagir, gerar dados, navegar e estabelecer relações na rede, por meio de provedores de acesso pelos quais se realizam várias atividades como o correio eletrônico; a computação de longa distância, o comércio eletrônico, o lazer, a pesquisa e outros.

Nesse contexto, de inegável evolução das tecnologias, o avanço da internet e a constituição do ciberespaço carecem de uma análise jurídica, normativa, sociológica, cultural e até mesmo psicológica. Com a evolução dos recursos da internet, é oportuna a reflexão quanto aos insumos contributivos à cultura, acesso e democratização da informação, valorização da diversidade e o processo de inclusão digital.

Contudo, também é indispensável refletir sobre os problemas jurídicos decorrentes da massificação do uso da internet. Assim, o estudo crítico no entorno do tema da proteção de dados pessoais é relevante para o meio jurídico, sobretudo quando se trata de uma reflexão frente aos marcos regulatórios do ciberespaço e as repercussões do caso de vigilância em massa denunciado por Edward Snowden, um ex-agente da *National Security Agency (NSA)*, dos EUA.

A pesquisa desenvolve o método de análise do mapeamento crítico [1], analisando comparativamente a interação de diálogos sociais e institucionais nos Estados Unidos na

[1] O termo mapeamento pode ser entendido como uma versão devidamente revista de uma análise analógica sem maiores questionamentos, efetuada rente à realidade, ou em outras palavras, a forma de análise jurídica não implica qualquer proposição transformadora para o direito. Mapeamento é a tentativa de descrever em detalhes a

formação do *backlash* no caso *NSA vs. Edward Snowden*, relacionado à vigilância e monitoramento de dados e informações pessoais pela agência estadunidense. O mapeamento crítico proposto nessa pesquisa leva em consideração os marcos regulatórios para a governança da internet no Brasil, e que tenham por escopo assegurar a proteção jurídica do direito à privacidade, à inviolabilidade dos dados pessoais, em equilíbrio com o direito ao acesso à informação, sobretudo em relação ao tema do estudo, que se concentra na compreensão de que a violação do direito à privacidade e à proteção dos dados pessoais configura uma transgressão aos direitos humanos.

Com essas considerações, pretende-se buscar resposta à seguinte indagação: em que medida a norma jurídica brasileira esta adequada como resposta aos atos de vigilância e monitoramento de informações e dados pessoais dos usuários praticada pela *NSA – National Security Agency*?

A pesquisa tem como objetivos: (i) observar e mapear a interação de diálogos sociais e institucionais dos Estados Unidos na formação do *backlash* do caso *NSA vs. Edward Snowden*; (ii) observar e mapear os resultados da formação do *backlash* do caso *NSA vs. Edward Snowden* a partir do reconhecimento da violação do direito à privacidade e à proteção dos dados pessoais como violação de direitos humanos; (iii) observar e mapear as normas jurídicas brasileiras constituídas a partir da compreensão jurídica da internet e as repercussões do caso *NSA vs. Edward Snowden*.

E é justamente nesse contexto em que o estudo apresentado elucidará os conceitos fundamentais do ciberespaço, das perspectivas do direito à proteção de dados pessoais no ciberespaço, enfatizando a relação deste com o reconhecimento do direito à privacidade e à proteção dos dados pessoais como direitos humanos, a partir de uma análise do *backlash* do caso *NSA vs. Edward Snowden*.

microestrutura juridicamente definida da sociedade com relação a seus ideais também articulados juridicamente. O segundo momento desta prática de análise deve ser chamado de crítica, isto é, uma versão revisada do que os juristas racionalistas desprezam como sendo a transformação da análise jurídica em conflito ideológico. Sua tarefa é explorar em detalhe as relações entre os arranjos institucionais da sociedade tais como representadas pelo direito, e os ideais ou programas professados por esses arranjos institucionais, na medida em que são frustrados ou cumpridos. (tradução nossa). (UNGER, 1996, p. 130).

1 INTERNET, CIBERSPAÇO E SOCIEDADE: A VIOLAÇÃO DE DIREITOS E O USO DE DADOS PESSOAIS.

Os dados pessoais tornaram-se o 'petróleo da internet' (LEMOS, 2012). Nesse sentido, no novo contexto global e social com o avanço da tecnologia da informação e comunicação, é indispensável estabelecer um marco conceitual para 'ciberespaço'. De acordo com Lessig (2006), o conceito de ciberespaço, em si, varia rapidamente, sobretudo em razão da identidade evidenciada, no tempo e no espaço, de acordo com os objetivos de uso da rede pelos usuários.

Para exemplificar tal afirmação, Lessig (2006) refere-se ao discurso intitulado "Declaração de Independência para o Ciberespaço", proclamado logo após o rompimento da cultura bipolar, com o fim da Guerra Fria, pelo compositor do *Grateful Dead*, banda de Rock dos anos 1960, John Perry Barlow, que também é fundador da EFF – *Eletronic Frontier Foundation*, uma organização não governamental que tem como escopo a defesa dos direitos civis dos usuários da *Web*, no qual Barlow (1996, p.01) pronuncia: "Governos da Era Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do ciberespaço, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não tem soberania onde nos reunimos".

A partir disso, identifica-se a percepção sobre o que é o ciberespaço e sobre a regulação e a governança da rede, especialmente com respeito ao alcance de instrumentos normativos que assegurem a proteção jurídica do direito fundamental à inviolabilidade dos dados pessoais ou venham a assegurar a proteção de direitos humanos no ciberespaço e, por consequência, neutralizem o abuso de poder de empresas e governos sobre dados e informações.

Pela visão reproduzida por Barlow como um expoente de defesa de direitos civis no ciberespaço, o discurso não era apenas de que o ciberespaço não poderia ser regulado pelo governo – pois ele não poderia efetivamente fazê-lo. O ciberespaço, por natureza, nascera inevitavelmente livre. Os governos poderiam ameaçar, mas o comportamento não poderia ser controlado; leis poderiam ser aprovadas, mas elas não teriam efetividade. Logo, dentro do ciberespaço não havia escolha sobre que tipo de governo instalar, eis que ninguém poderia reinar. Por consequência, o ciberespaço se constituiria em uma sociedade de tipo muito diferente: sem definição e direção, mas construído de baixo para cima. A sociedade deste espaço seria uma entidade totalmente auto-organizada, livre de governantes e de intervenção política (LESSIG, 2006).

Diante disso, é relevante diferenciar conceitualmente a internet do ciberespaço. Nem todos que se conectam à internet visitam o ciberespaço. A internet é que o meio através do qual o e-mail é entregue e as páginas da *Web* são publicadas. É o meio utilizado para fazer compras online ou assistir a vídeos por *streaming*. A Google está na internet, assim como o Facebook, o Twitter e outras mídias sociais.

Entretanto, o ciberespaço representa algo mais. Embora construído dentro da estrutura da internet, ele proporciona uma experiência mais rica. O ciberespaço é algo como quando o usuário se vê completamente envolvido pela intimidade provocada por um conjunto de mensagens de bate-papo instantâneo ou como a complexidade dos *Massively Multiple Online Games* (MMOGs), jogos que possibilitam a vários participantes jogarem simultaneamente por meio da internet, estando em diferentes lugares do mundo, porém envolvidos conjuntamente pelo mesmo ambiente virtual: o ciberespaço do MMOG (LESSIG, 2006).

Alguns indivíduos inseridos no ciberespaço acreditam estar em uma comunidade; outros simplesmente confundem suas vidas com sua existência no ciberespaço por meio de um avatar. Naturalmente, nenhuma linha nítida divide ciberespaço e internet. Há, porém, uma diferença importante na experiência com os dois. Possivelmente aqueles usuários que percebem a internet simplesmente como uma espécie de 'páginas amarelas' não reconhecerão o que os 'cidadãos do ciberespaço', como o mencionado ativista John Perry Barlow, falam e defendem. Para aqueles, o ciberespaço é algo obscuro ou simplesmente não existe (LESSIG, 2006).

Nesse contexto, percebe-se que, ao longo da história, as redes de comunicação foram criadas e aprimoradas, chegando ao patamar da criação de redes interligando computadores. A partir dessas redes foi constituída uma rede mundial de computadores, denominada internet. No princípio da década de 1990, a internet recebeu inovações para edição, acesso e compartilhamento de informações, dados e conteúdos, a partir dos protocolos da *World Wide Web*, adquirindo a partir de então a denominação '*Web'*. Na atualidade, rede, internet e *Web* correspondem ao mesmo meio utilizado para editar, publicar, compartilhar, armazenar e transmitir informações, dados, conteúdo e comunicação. Em uma conceituação mais profunda, o ciberespaço corresponde à interação mais intensa no uso dos recursos disponíveis para acesso via internet, estabelecendo uma organização social à parte, denominada de modos diversos, como se explicita a seguir.

1.1 A sociedade da relevância, o Estado de vigilância e a *surveillance*

Contemporaneamente, outras definições têm surgido como uma maneira de propor novos olhares sobre o que se reconhece como espaço gerado pela internet. A pesquisa identificou, na literatura recente, a atribuição de novos conceitos associados às transformações sociais causadas pela internet na sociedade em rede e na sociedade da informação.

Brito e Longhi (2014) defendem que a sociedade da informação está prestes a ser superada por um novo modelo de sociedade, denominado 'sociedade da relevância'. Para sustentar a tese, os autores reportam-se ao cenário descrito por Pariser (2012), em que as organizações dos segmentos de mídia, tecnologia, comunicação e conteúdo interativo passaram a perceber que, com o crescimento cada vez mais intenso de dados e informações na *Web*, ainda que indexados e organizados por motores de busca, como o Google, a escolha da informação pelo usuário de internet tornou-se um problema. A solução veio com a criação de filtros capazes de coletar dados pessoais de navegação do usuário, possibilitando atrair a atenção do leitor pela oferta de conteúdo customizado, alinhado a seus interesses pessoais. Os filtros estabeleceram uma nova maneira de buscar e de encontrar informação na *Web*, utilizando a relevância dos resultados como maneira de estabelecer a rede entre o usuário e a fonte do conteúdo procurado.

Todavia, esta pesquisa não localizou outros estudos e fundamentos que sustentem a tese de Brito e Longhi (2014). Por isso, é categórico afirmar que ainda não ocorreu a dita superação de um modelo social. Acredita-se, por outro lado, que a sociedade da informação vivencia uma geração distinta daquela que originou sua conceituação genuína. Logo, poderia se falar em sociedade da informação 2.0 ou 2ª geração da sociedade da informação, mas não de sua superação por uma sociedade da relevância, sobretudo por ser a relevância um método inserido nos códigos de programação dos *softwares* que fazem o tratamento dos dados, do conteúdo, das informações e das comunicações que circulam na rede, oferecendo ao usuário resultados diferentes, conforme seu perfil. Portanto, a informação ainda é o elemento preponderante do modo de organização social vivenciado na contemporaneidade.

Outra atribuição conceitual identificada reside na definição de "Estado de vigilância", defendida por Molinaro e Sarlet (2014, p. 30). De acordo com estes autores, assim como a sociedade em rede representa um novo modelo de sociedade, o Estado de vigilância

representa um novo modelo de Estado dentro da sociedade em rede, que consistiria em uma "forma de contaminação da democracia caracterizada pela intrusão dos governos e das corporações na liberdade e na privacidade de terceiros, sejam estes atores públicos ou privados".

Os mencionados doutrinadores brasileiros reproduzem uma análise realizada por Balkin (2008), que reporta à criação de um "Estado Nacional de Vigilância" como um método de reação ao eventos que compuseram os ataques terroristas de 11 de setembro de 2001, nos Estados Unidos. Para Balkin (2008), o governo estadunidense passou a utilizar a mineração de dados como um modo de analisar grandes volumes de dados, informações, conteúdos e comunicações.

Recentemente, Bauman e Lyon (2013) apresentaram uma análise relevante sobre esse contexto, sob o prisma do conceito de vigilância líquida. Para tais autores, a vigilância constitui uma dimensão elementar no mundo moderno. Em muitos países, as pessoas estão bastante conscientes sobre a maneira como o monitoramento em massa afeta suas vidas no dia a dia, pois as câmeras estão visíveis a todos, em diversos lugares públicos, não apenas em Nova Iorque ou Londres, mas também em Nova Déli, Shangai e Rio de Janeiro. Houve também, pós o '11 de setembro', a proliferação de um aparato tecnológico para controle de passaportes e identificação pessoal por dados biométricos, assim como de escâneres corporais, capazes de revelar, em uma inspeção de segurança, os detalhes mais íntimos do corpo humano.

A vigilância líquida debatida pelos autores não é tanto um modo integral de definir o monitoramento em massa como um meio para orientar ou situar as mudanças nela ocorridas dentro da modernidade líquida, fluída e inquietante que se vivencia na atualidade. Trata-se de uma vigilância que adotou a otimização de dados, informações, comunicações e conteúdos para aproveitá-los nos mais diversos segmentos, seja no âmbito da segurança, seja no âmbito do consumo. Assim, *bits* de dados pessoais são obtidos para determinado fim e utilizados com absurda facilidade para outros diversos objetivos públicos e privados, o que confere à vigilância o alcance de formas antes não imaginadas, respondendo à liquidez e à reprodução desses meios como instrumentos legítimos para a sociedade (BAUMAN; LYON, 2013).

O conceito de Estado de vigilância defendido por Balkin (2008) e corroborado por Molinaro e Sarlet (2014) tem como elementos característicos a coleta, o agrupamento, o tratamento e a análise de dados com a intenção de identificar 'potenciais ameaças' à

segurança nacional, bem como administrar e prestar serviços sociais com maior eficiência, pela otimização do uso das informação. Por essa razão, é possível dizer que o Estado de vigilância encontra-se sob o pálio da sociedade da informação.

De acordo com Morais e Neto (2014, p. 419),

> A categorização dos seres humanos tem como finalidade a sua inclusão ou exclusão em determinados grupos. E, com isso, uma nova categoria entra em cena, a *surveillance*, a qual levanta barreiras virtuais, capazes, assim, de garantir ou impedir o acesso aos elementos indispensáveis para uma vida digna, como, por outro lado, permitir novas formas de gestão e controle de pessoas, empresas, governos etc. E os critérios para a obtenção e uso dessas classificações, ressalte-se, não se submetem aos tradicionais controles e limites democrático-territoriais, sendo geridos, tratados e utilizados a partir da ideia de segredo: seja de Estado, seja comercial, visto que tais informações e as análises que delas derivam são consideradas propriedade da empresa que as obtém e oferece o serviço.

Afirmam os autores que o contexto atual permite evidenciar uma categoria nova, dotada de maior complexidade que a vigilância. Assim, "(…) A mera tradução da palavra *surveillance* como 'vigilância' é inadequada para englobar um fenômeno tão complexo, afinal, não se está falando de um evento especifico dirigido contra um sujeito determinado (como é o caso da vigilância) (...)" (MORAIS; NETO, 2014, p. 420).

De acordo com a visão de Morais e Neto (2014), um dos elementos centrais para a caracterização da categoria *surveillance* reside no uso de dados pessoais indexáveis, cujas informações são processadas para diferentes fins. Assim, o armazenamento e o processamento ilimitado desses dados e informações em tempo real – características presentes na geração de tecnologias da informação e comunicação da atualidade – são fundamentais para a configuração do conceito de *surveillance.*

Nessa esteira, é oportuno fazer menção ao movimento *Cypherpunk*, capitaneado contemporaneamente por Julian Assange e a organização por ele fundada, o *Wikileaks*. O referido movimento defende abertamente a utilização da criptografia e de métodos semelhantes como recurso para promover mudanças sociais e políticas, de modo a burlar o Estado de vigilância, já que a criptografia seria o recurso adequado para a defesa contra o uso de técnicas de monitoramento e vigilância da navegação na internet (ASSANGE, 2013).

Um dos exemplos observado, com frequência, quanto ao Estado de vigilância, em uma sociedade oriental, está no caso da China, que utiliza da tecnologia da *Deep Packet Inspection*

(DPI)[2] para promover o bloqueio arbitrário e a filtragem de conteúdo. Recentemente, o governo chinês foi 'vítima' de uma manobra sintática que burlou os filtros que impossibilitavam a visualização de uma célebre imagem do episódio histórico conhecido como "Massacre da Praça da Paz Celestial". Os cidadãos chineses que pesquisaram no dia 04 de junho de 2013 pelas expressões *Big Yellow Duck* passaram a ter acesso à imagem de um modo diverso do habitualmente bloqueado pela inspeção profunda de pacotes. Como resultado, os usuários de internet chinesa encontraram a imagem mostrada na ilustração 1 comparada à imagem original.

Ilustração 1: A China e o caso *Big Yellow Ducks*

Fonte: Adaptado de Tatlow (2013).

Como um modo de reconhecer o livre acesso à internet como um direito humano, a Organização das Nações Unidas emitiu o Relatório A/HRC/17/27, apresentado na décima sétima sessão do Conselho de Direitos Humanos da Assembleia Geral, intitulado "Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e de expressão", que levou em consideração atos de países que promoveram as seguintes ações:

[2] A *DPI* é um recurso tecnológico com o objetivo de gerenciar o tráfego de rede. Esse recurso possibilita que operadoras de rede realizem a análise profunda – por isso a denominação 'inspeção' é utilizada – dos pacotes de dados que transitam na infraestrutura de rede dessas operadoras, com uma finalidade primária de otimização dos custos, a partir do conhecimento do tráfego demandado pelos usuários. Assim, seria possível identificar quais serviços usados pelo usuário demandam maior banda de rede, ou seja, se determinado usuário utiliza a *Web* para navegação em *sites*, ou para assistir vídeos, ou acessar redes sociais. A adoção da *DPI* possibilitaria às operadoras fornecerem um serviço melhor qualificado ao consumidor (GEERE, 2012). Como bem refere Barretto (2013, p. 313), "(...) O lado ameaçador da técnica existe não só quando ocorre o abuso dela por má vontade, mas também quando ela é empregada de boa vontade para fins próprios legítimos. Ocorre o que Boudon chamou de 'efeitos perversos' da ação social".

bloqueio arbitrário ou a filtragem de conteúdo[3]; criminalização de expressão legítima; imposição de responsabilidades intermediárias; interrupção do acesso à internet pela população, fundamentada na violação de propriedade intelectual; ciberataques; e proteção inadequada (ou insuficiente) do direito à privacidade e à proteção dos dados pessoais (RUE, 2011).

Observa-se, nas imagens contidas na Ilustração 1, o uso da internet de forma criativa para burlar uma violação ao livre acesso à internet, principalmente como forma de controle pela força e pelo poder em Estados não democráticos, o que, na visão da Organização das Nações Unidas, configura-se como uma violação de direitos humanos. O Relatório da ONU identificou manifesta transgressão dos direitos humanos, sobretudo daqueles previstos no artigo 19 da Declaração Universal dos Direitos Humanos, interpretando-se sua extensão aos atos relacionados à internet, "Toda pessoa 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" (RUE, 2011, p.01, tradução nossa).

Percebe-se, na atuação de governos, a aplicação de um denominado 'poder potencial', que consiste "[...] naquele que tem a capacidade de modificar o comportamento do outro, sendo, portanto, relação entre atitudes de quem tem a possibilidade de exercer o poder e as do sujeito passivo" (MORAES FILHO, 2009, p. 641).

[3] Justamente nesse sentido, argumenta Monteiro (2013, p.01), em pesquisa desenvolvida pelo Observatório da Internet no Brasil, que a *DPI* é um recurso tecnológico cujos benefícios são altamente questionáveis, por permitir que provedores de acesso à internet obtenham os dados pessoais dos usuários e monitorem sua utilização da rede. Para a pesquisadora, a identificação do tráfego dos usuários poderia provocar "[…] ações desejadas pelo poder público, como controle de conteúdos acessados por cidadãos (censura), ou orientar interesses empresariais, como diferenciação de tráfego para serviços pouco desejados e competitivos aos seus serviços", o que já ocorre em países com regimes governamentais democráticos e não democráticos. Exatamente nesse aspecto reside a controvérsia sobre a Recomendação *ITU-T* Y.2770 (INTERNATIONAL TELECOMMUNICATION UNION, 2012) que estabeleceu os requisitos de utilização da *DPI* nas próximas gerações de redes. Esse documento foi objeto de discussão e deliberação na *World Telecommunication Standardization Assembly,* realizada em Dubai, no final de 2012, dele resultou um tratado que não foi assinado por 55 países-membros, dentre os quais Alemanha, Canadá, Estados Unidos, Chile, Colômbia, Reino Unido e Suécia (MONTEIRO, 2013).

2 UMA ANÁLISE DA VIOLAÇÃO DE DADOS PESSOAIS NA INTERNET A PARTIR DO CASO NSA VS. EDWARD SNOWDEN

A tese de sustentada por Balkin (2008) e denunciada por Assange (2013), evidenciada no exemplo de uso da *Deep Packet Inspection* pelo governo chinês, ganhou mais força e repercussão, em junho de 2013, quando o jornal britânico *The Guardian* noticiou, com exclusividade, a primeira matéria de uma série organizada e assinada pelo jornalista Glenn Greenwald sobre os programas de espionagem mantidos pela *NSA – National Security Agency*, a Agência Nacional de Segurança dos Estados Unidos. Ela realizava a coleta de dados de ligações telefônicas de cidadãos americanos e de fotos, *e-mails* e videoconferências de usuários vinculados aos serviços de internet fornecidos por empresas americanas, como Google, Facebook e Microsoft/Skype. Na sequência de reportagens, o jornal divulgou ao mundo que o colaborador das matérias era Edward Snowden, um ex-funcionário de uma empresa que prestava serviços à *NSA*. As informações entregues por Snowden possibilitaram detectar a existência de um sistema de vigilância secreto, denominado *XKeyscore,* o qual permitiria aos órgãos de inteligência dos EUA supervisionar ações de rotina comuns à maior parte dos usuários de internet no mundo (GREENWALD, 2013).

Não bastasse tal revelação, em outubro, o jornal *Washington Post* noticiou que a *NSA* teria realizado uma invasão secreta aos *links* de conexão aos *data centers*[4] das empresas de tecnologia Yahoo e Google, em diversos países, tendo acesso a dados de expressivo número de contas de usuários, e também que os órgãos de inteligência estadunidenses fariam o monitoramento diário da localização geográfica de centenas de milhões de celulares no mundo todo (GELLMAN; SOLTANI, 2013).

O jornal brasileiro "O Globo" publicou, em julho de 2013, uma matéria intitulada "EUA espionaram de *e-mails* e ligações de brasileiros"[5], referindo que brasileiros usuários de

[4] Correspondem aos centros de processamento de dados, onde geralmente estão situados os servidores que armazenam dados e informações.

[5] A questão envolvendo a NSA e a coleta de dados e informações pessoais singulares e de governos, inevitavelmente, adentra o tema da soberania dos Estados. Contudo, esta pesquisa não tem como pretensão aprofundar o tema vinculado à teoria do Estado, visto que o objeto da pesquisa concentra-se na demonstração de vulnerabilidades na proteção de dados pessoais na internet, no âmbito do direito brasileiro. Assim, ao tratar do tema da vigilância em massa e da *surveillance*, a pesquisa pretende apenas sinalizar as respostas institucionais já apresentadas como modos de solução dos episódios de vigilância realizados pela NSA, convergindo para a tratativa do tema da proteção dos dados pessoais e não para a crise conceitual da soberania dos Estados.

internet, membros do governo, empresas de segmentos-chave tinham sido vítimas do monitoramento proposto pelos programas da *NSA* (GREENWALD; KAZ; CASADO, 2013).

O caso em questão é um exemplo típico de formação de um *backlash* em âmbito mundial, adstrito à constatação da existência de um Estado de vigilância, por conta da evidente violação constitucional, seja no contexto do direito constitucional brasileiro, seja no da jurisdição norte-americana. A resposta para conflitos e violações de direitos dessa natureza costuma ser uma resposta constitucional, já que, nas palavras de Oliveira e Oliveira (2011, p. 105), "o caso fica por conta da compreensão da Constituição, da disputa entre direitos nela sempre abrigados (expressa ou implicitamente), o que não levaria ao ônus mais severo, drástico, de romper com ela, ou seja, romper com a tradição, com a história constitucional".

Em conformidade com Post e Siegel (2007), a expressão *backlash* representa a concepção de reação contrária a uma medida ou decisão estatal, significando expressiva resistência, oposição jurídico-política de considerável intensidade sobre o caso em si, como se observa em *NSA versus* Edward Snowden.

O caso *NSA versus* Edward Snowden provocou o estabelecimento do que Oliveira e Oliveira (2011) definem como diálogos institucionais, por meio das interações entre os poderes executivo, legislativo e judiciário, e como diálogos sociais, intermediados pela reação de atores sociais sob uma estrutura *multistakeholder* (usuários de internet, ativistas, empresas, pesquisadores, organizações não governamentais).

De acordo com Oliveira e Oliveira (2011, p. 124), um *backlash* se forma por três elementos: a decisão ou medida estatal levanta uma questão controversa; a decisão ou medida estatal levanta um sentimento de desconforto, irresignação, resultante da interferência externa; a decisão ou medida estatal levanta uma subversão da ordem natural/política da mudança/afirmação da sociedade pelo envolvimento determinante do judiciário.

No contexto norte-americano, muitas foram as reações vinculadas ao caso *NSA versus* Edward Snowden. Inicialmente os atores sociais, por meio de diversas organizações não governamentais de defesa de direitos e liberdades civis, como a *Eletronic Frontier Foundation,* a *Global Network Initiative* e a *American Civil Liberties Union,* manifestaram-se em repúdio às medidas adotadas pelos órgãos de espionagem vinculados à *NSA*.

Após a grande repercussão relacionada ao caso, as maiores empresas de tecnologia do mundo – *AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter e Yahoo* – apresentaram um manifesto denominado *Global Government Surveillance Reform*, no qual

sugerem um novo modelo de coleta e tratamento das informações dos usuários de internet. Em síntese, são propostos cinco princípios fundamentais: limitação da coleta de informações dos usuários pelos governos; fiscalização e prestação de contas; transparência sobre as exigências de governos; respeito ao livre fluxo de informações; evitar conflitos entre governos. (REFORM GOVERNMENT SURVEILLANCE, 2013).

Além dessas manifestações, foi constituída, nos EUA, a coalizão de *policy makers* OFF NOW, com o objetivo de promover a criação legislativa nos Estados americanos, bloqueando (ou até mesmo 'anulando') o prosseguimento das ações da *NSA,* tais como denunciadas por Edward Snowden. Até a data de 10 de janeiro de 2014, cinco Estados americanos (Califórnia, Arizona, Missouri, Kansas e Oklahoma) já haviam recebido propostas introduzidas por senadores do que a coalizão denomina de "*Fourth Amendment Protection Act*" (OFF NOW, 2014).

Na prática, a proposta legislativa tem como objetivos proibir as agências estaduais e locais de prestar qualquer apoio material à *NSA* sob sua jurisdição, inclusive através de utilitários de propriedade do governo, de fornecimento de água e de eletricidade; fornecer informações recolhidas sem mandado pela *NSA* e compartilhados com a aplicação da lei inadmissível em um tribunal estadual; impedir universidades públicas de servirem como centros de pesquisa ou meio de recrutamento da *NSA;* aplicar sanções contra empresas que tentam preencher necessidades não atendidas na ausência de cooperação do Estado (MAHARREY, 2014).

Como efeito das iniciativas dos atores sociais, dois cidadãos norte-americanos propuseram a ação civil nº 13-0851 (caso *Klayman et al. versus Obama et al.*), perante a Corte do Distrito de Columbia, com o objetivo de impedir a coleta de dados e informações pessoais dos usuários pelos programas da *NSA*, bem como de solicitar a destruição de todos os dados coletados até então. Em 16 de dezembro de 2013, o juiz federal Richard Leon deferiu a liminar pleiteada pelos requerentes afirmando, dentre outros fatores indicados na extensa decisão, que o programa de vigilância do governo dos Estados Unidos, a partir de metadados, constitui uma violação dos direitos de privacidade, ferindo a quarta emenda da Constituição. O juiz diz, em sua decisão, ter "dúvidas sobre a eficácia do programa de coleta de metadados como um meio de conduzir investigações sensíveis em casos que envolvam ameaças iminentes de terrorismo" (DISTRITO DE COLÚMBIA, 2013).

Com objetivos similares à ação anteriormente mencionada, foi proposta a ação civil n.º 13-3994 (caso *American Civil Liberties Union et al. versus James R. Clapper et al.*) perante a Corte do Distrito de Nova York. Entretanto, diferentemente da decisão do juiz Leon, o despacho liminar do juiz federal William Pauley, publicado em 27 de dezembro de 2013, concluiu que a coleta de metadados pelos programas de vigilância da *NSA* está dentro da lei e não viola o direito de privacidade dos cidadãos norte-americanos, pois não haveria provas de que a agência teria utilizado esses dados para outras finalidades que não a investigação de ataques terroristas. Para o julgador, trata-se da aplicação da razoabilidade na interpretação da Quarta Emenda à Constituição estadunidense (DISTRITO DE NOVA YORK, 2013).

Após as decisões dos dois casos, as partes sucumbentes interpuseram recurso e os casos devem, em breve, estar na Suprema Corte dos EUA, que conferirá a 'resposta constitucional'. É indispensável considerar a afirmação de Bateup (2006) de que, quando realizado o exercício do poder de revisão judicial, os juízes se envolvem em um diálogo interativo, interconectado e dialético sobre os significados constitucionais. Assim, os julgamentos constitucionais são, ou deveriam ser, produzidos por meio de um processo de elaboração compartilhada entre o judiciário e outros atores constitucionais (BATEUP, 2006). Indubitavelmente, no caso *NSA versus* Edward Snowden há uma reação diversificada no amplo exercício dos diálogos institucionais e sociais para a formação de um *backlash*.

Observa-se, contudo, que as reações aos diálogos institucionais identificados por essa pesquisa vão de encontro à solução proposta por Assange. Ele sugere que o único caminho para superar o Estado de vigilância sustentado por Balkin é o uso da criptografia, ou seja, da mais alta tecnologia para uso anônimo de recursos, dados, informações e conteúdos que trafegam na internet. Trata-se, portanto, de uma resposta não institucional típica do movimento *hacker* em uma geração mais recente representada pelos *cypherpunks.*

Conforme a visão dos autores referenciados nessa pesquisa, o Estado de vigilância representa uma nova formatação da organização de Estado. Ele adota parâmetros e tecnologias que utilizam as redes, em especial a internet no modelo vigente de protocolo *Web*, para promover o monitoramento e a coleta de dados, informações, comunicações e conteúdos, para atingir diferentes fins, em especial, o de estabelecer estratégias de segurança nacional. A conceituação de Estado de vigilância não se confunde com os conceitos de internet, *Web*, rede, ciberespaço, sociedade em rede e sociedade da informação, visto que essa nova

formatação de Estado corresponde à reformatação do modelo anterior com o aproveitamento dos insumos trazidos por diferentes conceitos.

2.1 O Direito brasileiro e as repercussões do caso *NSA vs. Edward Snowden*

Diferentemente do que ocorreu nos Estados Unidos, no contexto brasileiro não houve a formação de um *backlash* com o desenvolvimento de diálogos institucionais advindos da repercussão do caso de vigilância em massa denunciado por Edward Snowden. Contudo, o Direito brasileiro já se apresenta dotado de algumas normas jurídicas que, em certa medida, atendem aos anseios jurídicos da sociedade, embora muitas outras se distanciem de uma compreensão jurídica da internet.

A Constituição Federal de 1988[6] é cristalina ao reconhecer, como direitos fundamentais, a inviolabilidade da intimidade, da vida privada, da honra e a imagem das pessoas, restando assegurado o direito à reparação pelos danos materiais ou morais decorrentes de sua violação. Nesse mister, também é sabido que o artigo 5º, inciso XII, inclui, no rol de direitos fundamentais, a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, excetuando as hipóteses vinculadas à produção de provas em investigação criminal ou instrução processual penal.

Diversas normas jurídicas brasileiras mantêm distanciamento de situações vinculadas aos novos fenômenos proporcionados pela internet, na sociedade da informação, tais como o Código de Defesa do Consumidor, o Código Civil, a Lei do *Habeas Data* (Lei n.º 9.507/97), a Lei Complementar n.º 105/2001 (que trata do sigilo sobre operações financeiras) . Apenas a título exemplificativo e de modo a estabelecer uma relação entre as normas constitucional, consumerista, bancária e civilista, respectivamente, cita-se o caso observado em recente estudo desenvolvido no Instituto de Tecnologia de Massachussets, publicado por De Montjoye et al. (2015) na revista *Science*.

[6] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

O estudo intitulado "*Unique in the shopping mall: On the reidentifiability of credit card metadata*" apresentou o desenvolvimento de um algoritmo matemático que, instalado dentro do sistema informacional de uma instituição financeira, foi capaz de coletar metadados anônimos, armazenados sob sigilo, obtidos a partir de compras realizadas com cartões de crédito, em estabelecimentos comerciais. De acordo com os resultados da pesquisa, foi possível identificar um consumidor pela coleta de dados de, em média, quatro operações financeiras com cartão de crédito (DE MONTJOYE et al., 2015).

Destarte, metadados anônimos e até mesmo protegidos por normas de sigilo bancário, tal como prevê a lei brasileira, tornam-se dados pessoais vulneráveis, eis que passíveis de identificação da pessoa em questão, ainda que sujeitos às proteções legais, especialmente as relacionadas com a tutela constitucional e civilista da vida privada. Abrem-se, com isso, diversas possibilidades de registro e tratamento dos dados, inclusive de maneira ilícita, por governos, empresas e indivíduos. Apesar da tutela constitucional e infraconstitucional mencionada, acredita-se na necessidade de melhor compreensão da internet no âmbito jurídico, de modo a conferir maior eficácia à proteção dos direitos fundamentais, conforme se vê a seguir.

2.1.1 A tutela da proteção de dados pessoais em um contexto constituído a partir de uma compreensão jurídica da internet

Diferentemente das normas jurídicas mencionadas anteriormente, o ordenamento jurídico brasileiro recepcionou, recentemente, três legislações que passaram a tutelar direitos, considerando a internet como um ambiente merecedor de reconhecimento normativo, com a vigência da Lei de Acesso à Informação (LAI), em 2011; da Lei de Crimes Informáticos (LCI), em 2012; do Marco Civil da internet (MCI), em 2014. Além dos referidos diplomas legais, é relevante considerar, no contexto desta pesquisa, o anteprojeto de lei de proteção de dados pessoais em discussão no Brasil.

A partir da vigência da Lei n. 12.527/2011, popularmente conhecida como Lei de Acesso à Informação, foi regulamentado o acesso a informações, previsto nos artigos 5º, inciso XXXIII, e 37, parágrafo 3º, inciso II, e 216, parágrafo 2º da Constituição Federal. Estão subordinados à referida lei os órgãos públicos que fazem parte da administração direta dos Poderes Executivo, Legislativo, Judiciário, incluindo-se os Tribunais de Contas e o Ministério

Público, bem como autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais instituições sob o controle direto ou indireto da União, dos Estados, do Distrito Federal e dos Municípios, com aplicação estendida às instituições privadas sem fins lucrativos que desenvolvam ações de interesse público e recebam recursos públicos (BRASIL, 2011).

Salienta-se que a Lei de Acesso à Informação destina-se a assegurar o direito fundamental de acesso à informação, observando princípios básicos da administração pública, tais como observância da publicidade como preceito geral, sendo o sigilo uma exceção; divulgação de informações de interesse público; utilização de meios de comunicação facilitados pela tecnologia da informação; entre outros (BRASIL, 2011).

O direito ao acesso à informação, assegurado pela norma jurídica em questão, é um mecanismo de fortalecimento da democracia e da participação política. Assim, o acesso à informação é um requisito prévio para a plena democracia, uma vez que é indispensável que os cidadãos estejam informados ou que tenham conhecimento suficiente sobre o seu objeto de participação no sistema democrático (GALINDO AYUDA, 2012).

Sob o prisma conceitual, a Lei de Acesso à Informação representa significativo avanço para o ordenamento jurídico brasileiro, já que apresenta um rol de definições que se mostra atual e contemporâneo. Destacam-se as definições conferidas aos termos ‘informação’, ‘informação pessoal’ e ‘tratamento da informação’, por estarem diretamente vinculadas ao tema desta pesquisa. No âmbito dessa lei, compreende-se por ‘informação’ os “(...) dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”. A definição para ‘informação privada’ corresponde àquela “(...) relacionada à pessoa natural identificada ou identificável”. O conceito de ‘tratamento da informação’ identifica “(...) conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação” (BRASIL, 2011).

A Lei de Acesso à Informação determina que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, o que, nos fundamentos defendidos nesta pesquisa, corresponde à proteção do direito fundamental à privacidade. A lei impõe restrições substanciais de acesso a

informações pessoais, como o acesso restrito às informações, pelo prazo máximo de cem anos, a agentes públicos autorizados, bem como a possibilidade de acesso ou divulgação a terceiros, mediante prévio consentimento do titular das informações, exceto nos casos previstos no regulamento.

A segunda norma jurídica brasileira contemporânea a recepcionar o contexto da internet é a Lei n. 12.737/2012, conhecida também como Lei de Crimes Informáticos, que alterou e incluiu dispositivos no Código Penal brasileiro. Em que pese a norma e a matéria não tenham relação direta com o tema de pesquisa desenvolvido nesta pesquisa, destaca-se o emprego de terminologias afins, as quais são tratadas de modo especial neste capítulo. Exemplo disso é o artigo 154-A, incluído no texto do Código Penal, que tipificou o crime de invasão de dispositivo informático como o ato de "(...) Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2012).

Depreende-se do diploma legal, que tutela os crimes informáticos, a preocupação do legislador em conferir maior proteção na seara penal aos dados, estendendo a compreensão do crime de invasão de dispositivo informático à obtenção, à adulteração, ou à destruição de dados e informações do titular do dispositivo, sem seu consentimento expresso ou tácito. Contudo, o legislador imprimiu à Lei de Crimes Informáticos uma economia textual desnecessária, não expressando questões relacionadas aos conceitos e às definições fundamentais para a aplicação da norma.

O terceiro diploma legal advindo de um cenário normativo contemporâneo, no Brasil, é a Lei n. 12.965/2014, popularmente denominada Marco Civil da Internet. Esta norma jurídica foi constituída após amplo debate colaborativo, em um processo pioneiro em âmbito global, instituindo uma carta de direitos para a internet no Brasil.

No que diz respeito ao tema desta pesquisa, assinala-se a importância do Marco Civil da Internet. Conforme observado no rol normativo – anterior à compreensão jurídica da internet até o advento do Marco Civil – o acesso aos dados e o registro da conduta de seus usuários eram plenamente destituídos de regulação específica, o que também permitiu que a internet se tornasse um ambiente hostil e de cometimento de abusos e violações de direitos. Um exemplo disso está na coleta deliberada de dados sigilosos, tanto em relação às informações quanto ao

histórico de navegação em *sites* da internet, bem como a frequente solicitação de tempo e conteúdo por autoridades públicas sem submissão à prévia análise judicial (LEMOS, 2014).

Nesse ponto específico, o Marco Civil representa o maior avanço normativo diretamente vinculado ao uso da internet na vida civil brasileira. Ele trouxe consigo algumas das respostas legislativas que contribuem para o fortalecimento do Estado Democrático de Direito e, principalmente, do reconhecimento de direitos e de sua extensão para a internet.

Inevitavelmente, a instituição do Marco Civil da Internet também trouxe ao meio jurídico o debate sobre a necessidade de uma norma jurídica que recepcionasse e reconhecesse direitos, dentro do contexto da internet no Brasil. Nesse ponto, a visão de Streck (2014, p. 335), sobretudo sob o viés da Crítica Hermenêutica do Direito, é esclarecedora:

> […] concordo que, em muitos casos, as novas leis são desnecessárias e não contribuem para uma configuração sistemática do nosso direito. No entanto, entendemos que isso não se aplica ao Marco Civil da Internet, se compreendermos a sua importância a partir da necessidade de se regulamentar o uso da internet no contexto brasileiro. Isso porque a Lei Geral de Telecomunicações, Lei 9.472/97, tem-se mostrado insuficiente, uma vez que regulava uma realidade em que a internet não estava tão presente no cotidiano dos brasileiros como hoje, de forma que uma série de novos problemas surgiram, acompanhando o desenvolvimento tecnológico. Assim, é evidente que o estabelecimento de alguns parâmetros para a regulamentação do uso da internet no Brasil é um importante avanço para o devido tratamento jurídico das mais diversas relações sociais dela decorrentes no país.

O Marco Civil da Internet representou um significativo avanço no panorama normativo brasileiro, particularmente por recepcionar a compreensão jurídica da internet. Mais do que estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabeleceu que a disciplina do uso da internet no Brasil tem como fundamentos o respeito à liberdade de expressão; o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; a finalidade social da rede (BRASIL, 2014).

O MCI também consagrou princípios elementares para a regulamentação civil do uso da internet no Brasil. Assim, a disciplina de seu uso no país deve seguir os princípios da garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; da proteção da privacidade; da proteção dos dados pessoais, na forma da lei; da preservação e garantia da neutralidade de rede; da preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os

padrões internacionais e pelo estímulo ao uso de boas práticas; da responsabilização dos agentes de acordo com suas atividades, nos termos da lei; da preservação da natureza participativa da rede; da liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios previstos na lei (BRASIL, 2014).

O rol de direitos e garantias aos usuários de internet no Brasil é um dos pontos fortes do Marco Civil da Internet, pois confere maior eficácia a direitos fundamentais já consagrados no ordenamento jurídico brasileiro, antes mesmo do advento da internet.

A carta de direitos da internet brasileira assegura aos usuários o acesso a ela como um elemento essencial ao exercício da cidadania, adotando a garantia do direito à privacidade e à liberdade de expressão nas comunicações como uma condição para o pleno exercício do direito de acesso à internet. A referida norma jurídica também assegura a inviolabilidade e a proteção da intimidade e da vida privada, bem como a indenização pelo dano material ou moral decorrente de sua violação; a inviolabilidade e o sigilo do fluxo de suas comunicações pela internet, salvo determinação contrária por ordem judicial; a inviolabilidade e o sigilo das comunicações privadas armazenadas, salvo determinação contrária por ordem judicial; o não fornecimento a terceiros de dados pessoais, inclusive de registros de conexão e de acesso a aplicações de internet, exceto mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (BRASIL, 2014).

Observa-se, portanto, que o Marco Civil da Internet adianta-se no tratamento do tema da proteção dos dados na internet, exigindo que as informações sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais sejam claras e completas; sejam limitadas a finalidades que justifiquem a coleta; não sejam vedadas pela legislação; estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet (BRASIL, 2014).

No tocante à tutela da proteção dos dados pessoais na internet, o Marco Civil recepciona a exigência do consentimento expresso sobre a coleta, o uso, o armazenamento e o tratamento de dados pessoais, deve isto ocorrer de forma destacada das demais cláusulas contratuais. Abre também a possibilidade de exclusão definitiva dos dados pessoais que tiverem sido fornecidos para determinada aplicação de internet, a requerimento do interessado, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros elencadas na lei (BRASIL, 2014).

Ainda, no que tange à inviolabilidade de dados pessoais na internet como uma garantia do direito fundamental à privacidade, o Marco Civil determina que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

Nesse sentido, o provedor responsável pela guarda somente será obrigado a disponibilizar os registros, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, devendo proceder do mesmo modo em relação ao conteúdo das comunicações privadas (BRASIL, 2014).

Há outro ponto que representa evolução normativa para a tutela de direitos na internet e que responde, parcialmente, os frequentes questionamentos sobre a eficácia normativa de uma lei nacional, quando estão em xeque a soberania dos Estados e a característica transnacional da rede. Ele diz respeito à determinação de que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, devem ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, considerando que pelo menos um dos terminais esteja localizado no Brasil, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior (BRASIL, 2014).

Contudo, há diversos dispositivos do Marco Civil da Internet que deverão ser submetidos a regulamento próprio, por meio de decreto. Dentre estes estão as medidas e os procedimentos de segurança e de sigilo que devem ser informados, de modo claro, pelo responsável pela provisão de serviços, em atendimento aos padrões definidos em regulamento, respeitado o direito de confidencialidade quanto a segredos empresariais; a prestação de informações pelos provedores de conexão e de aplicações de internet, de modo a permitir a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como ao respeito à privacidade e ao sigilo de comunicações; o procedimento para a apuração de infrações e a aplicação das penalidades previstas no Marco Civil da Internet (BRASIL, 2014).

A discussão no entorno do tema do direito fundamental à proteção da privacidade e da inviolabilidade dos dados pessoais na internet não se encerra com o Marco Civil da Internet, nem com os decretos que regulamentarão os mencionados pontos. Este é um debate em construção a partir do levantamento de contribuições no portal "Pensando o Direito"[7], vinculado ao *website* do Ministério da Justiça brasileiro. Ademais, conforme se vê a seguir, no mesmo sentido foi desencadeado o processo de recepção de contribuições para um anteprojeto de lei de proteção de dados pessoais para o Brasil.

Ainda que não apresente aspectos explícitos relacionados à proteção da privacidade na internet, o anteprojeto de lei de proteção de dados pessoais no Brasil representa significativo avanço rumo à regulamentação da tutela dos dados. Do mesmo modo como vem ocorrendo com a regulamentação dos aspectos relacionados à privacidade e à proteção dos dados pessoais, previstos no Marco Civil da Internet, o anteprojeto de lei de proteção de dados pessoais também foi submetido a um debate a partir do levantamento de contribuições no portal "Pensando o Direito"[8], vinculado ao *website* do Ministério da Justiça brasileiro.

Como muito bem refere Doneda (2006, p. 326), "[…] a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada a esta, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento jurídico brasileiro", especialmente no que diz respeito às normas jurídicas formuladas antes da compreensão jurídica da internet.

Na forma como foi apresentado para consulta e contribuição pública, o anteprojeto de lei de proteção de dados pessoais tem como objetivo a aplicação da norma a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independente do país de sua sede e do país onde esteja localizado o banco de dados, desde que a operação de tratamento seja realizada no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional, excetuando-se os casos em que o tratamento dos dados foi realizado por pessoa natural para fins exclusivamente pessoais; ou realizados para fins exclusivamente jornalísticos (BRASIL, 2015).

[7] O debate sobre a regulamentação do Marco Civil da Internet recebeu contribuições até o dia 30 de abril de 2015, na plataforma Pensando o Direito (http://participacao.mj.gov.br/marcocivil/).
[8] O debate sobre a regulamentação do Anteprojeto de Lei de Proteção de Dados Pessoais recebeu contribuições até o dia 30 de abril de 2015, na plataforma Pensando o Direito (http://participacao.mj.gov.br/dadospessoais/).

Por análise comparativa das diretivas europeias destinadas à proteção de dados pessoais, verifica-se que o rol de definições do anteprojeto de lei de proteção de dados pessoais é significativo e consistente para abranger diversas hipóteses fáticas, relacionadas ao que o anteprojeto define como tratamento de dados. Observa-se também que o anteprojeto brasileiro recepciona o conceito do consentimento como um dos elementos de tutela dos dados pessoais.

De acordo com Doneda (2006, p. 375), a "[…] reflexão sobre o papel do consentimento para o tratamento de dados pessoais é necessária para retirá-lo de uma posição na qual, escorado na tecnicidade, ele poderia neutralizar a atuação dos direitos fundamentais". Assim,

> […] O consentimento para o tratamento dos dados pessoais toca diretamente elementos da própria personalidade, porém não dispõe destes elementos. Ele assume mais propriamente as vestes de um ato unilateral, cujo efeito é o de autorizar um determinado tratamento para os dados pessoais (DONEDA, 2006, p. 377-378).

Os princípios da finalidade estão diretamente vinculados ao conceito de tratamento de dados, o qual assegura que estes devem ser tratados com finalidades legítimas, específicas, explícitas e conhecidas pelo titular, indo ao encontro do princípio da transparência, que garante aos titulares informações claras e adequadas sobre a realização do tratamento. Complementarmente, o princípio da adequação sugere que o tratamento deve ser compatível com essas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento (BRASIL, 2015).

O princípio da necessidade ressalta que o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos, na mesma proporção em que o princípio da segurança determina que devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Nesse sentido, é fundamental a aplicação do princípio da prevenção, que determina a necessidade de serem adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, considerando os riscos existentes (BRASIL, 2015).

Destarte, o princípio do livre acesso garante a consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade de seus dados pessoais. Isto permite a aplicação do princípio da qualidade dos dados, que assegura a exigência de

exatidão, clareza e atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento, e a observância do princípio da não discriminação, que assegura a neutralidade no tratamento dos dados, o qual não pode ser realizado para fins discriminatórios, vinculando-se integralmente à preocupação manifestada no núcleo do anteprojeto, no que diz respeito aos dados sensíveis (BRASIL, 2015).

CONCLUSÃO

Na busca de resposta ao problema formulado, qual seja o de verificar em que medida a norma jurídica brasileira esta adequada como resposta aos atos de vigilância e monitoramento de informações e dados pessoais dos usuários praticada pela *NSA – National Security Agency,* a pesquisa cumpriu os quatro objetivos específicos.

A partir de uma construção teórica do contexto histórico e social da internet e do ciberespaço, foi possível observar e mapear a interação de diálogos sociais e institucionais dos Estados Unidos na formação do *backlash* do caso *NSA vs. Edward Snowden,,* bem como observar e mapear os resultados da formação do *backlash* do caso *NSA vs. Edward Snowden* a partir do reconhecimento da violação do direito à privacidade e à proteção dos dados pessoais como violação de direitos humanos.

Por outro lado, a partir da identificação e aprofundamento das normas jurídicas brasileiras, foi possível observar e mapear as leis brasileiras constituídas a partir da compreensão jurídica da internet em meio às repercussões do caso *NSA vs. Edward Snowden*.

Destarte, foi possível evidenciar que o ordenamento jurídico brasileiro, a partir da Lei de Acesso à Informação, da Lei de Crimes Informáticos e do Marco Civil da Internet, mantem grande proximidade com a compreensão jurídica da internet e seus efeitos para a vida em sociedade. Embora o Direito não seja a única resposta, assim como não será sempre a mais adequada, ao tutelar de modo específico temas como a proteção de dados pessoais, bem como aprofundar a proteção dos direitos fundamentais na internet, pode-se afirmar que tais leis representam uma resposta coerente e eficiente sobre os efeitos gerados a partir da repercussão do caso de vigilância em massa desenvolvido pela *National Security Agency*, dos EUA.

Evidentemente, o tema não se esgota com as evidências parciais e preliminares apresentadas neste estudo. Como abordado no último subtítulo, o Brasil ainda carece de regulamentações importantes no âmbito do Marco Civil da Internet, assim como urge a

instituição de uma lei geral de proteção de dados pessoais, especialmente no contexto da internet.

Em uma adaptação livre do trecho[9] da obra de Orwell (1983), "[…] ao futuro ou ao passado, a um tempo em que o pensamento seja livre […]",que, na internet ou fora dela, os homens sejam iguais, e que não vivam sós – a um tempo em que a verdade exista e que cada sujeito tenha a possibilidade de decidir quais de suas informações são privadas e quais são públicas, e em que o que for feito também possa ser desfeito: da era da navegação privada na internet, da era da *accountability* de quem monitora, da era do direito de deletar os dados pessoais, da era da proteção da identidade *online*, da era da privacidade na internet – saudações!

REFERÊNCIAS

ASSANGE, J. *Cypherpunks: Liberdade e o futuro da internet.* São Paulo: Boitempo Editorial, 2013.

BALKIN, J. *The Constitution in the National Surveillance State.* 2008.

BARBER, L. How a soccer star sparked the freedom debate of our age - FT.com. *The Financial Times*, 27 maio 2011.

BARLOW, J. P. *A Declaration of the Independence of Cyberspace.* Disponível em: <https://projects.eff.org/~barlow/Declaration-Final.html>. Acesso em: 23 fev. 2011.

BARRETTO, V. *O Fetiche Dos Direitos Humanos E Outros Temas.* Porto Alegre: Livraria do Advogado, 2013.

BATEUP, C. The Dialogic Promise: Assessing the Normative Potential of Theories of Constitutional Dialogue. *Brooklyn Law Review.* v. 71, p. 05–24, 2006.

BAUMAN, Z.; LYON, D. *Vigilancia líquida.* Madrd: Grupo Planeta Spain, 2013.

[9] Ao futuro ou ao passado, a um tempo em que o pensamento seja livre, em que os homens sejam diferentes uns dos outros, em que não vivam sós – a um tempo em que a verdade exista e em que o que for feito não possa ser desfeito: da era da uniformidade, da era da solidão, da era do Grande Irmão, da era do duplipensamento – saudações! (tradução nossa) (ORWELL, 1983).

BERNAL, P. A. Web 2.5: the symbiotic web. *International Review of Law, Computers and Technology*. v. 24, n. 1, p. 25–37, 1 mar. 2010.

BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 fev. 2014.

_____. *Lei n.º 12.527, de 18 de novembro de 2011*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 abr. 2015.

_____. *Lei n.º 12.737, de 30 de novembro de 2012*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 abr. 2015.

_____. *Lei n.º 12.965, de 23 de abril de 2014*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 abr. 2015.

_____. *Anteprojeto de Lei para a Proteção de Dados Pessoais*. Disponível em: <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 28 abr. 2015.

BRITO, A. U. DE; LONGHI, J. V. R. Diversidade e pluralidade como fundamentos do Marco Civil da Internet no Brasil e as bases axiológicas da democracia contemporânea. In: LEITE, G.; LEMOS, R. (Eds.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 79–92.

CASTELLS, M. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. [s.l.] Wiley, 2011.

_____. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge (UK): Polity Press, 2013.

COMITÊ GESTOR DA INTERNET NO BRASIL. *CGI.br - Resolução CGI.br/RES/2012/008/P*. São Paulo: [s.n.]. Disponível em: <http://www.cgi.br/resolucoes/documento/2012/008>. Acesso em: 3 jan. 2015.

DE MONTJOYE, Y.-A. et al. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*. v. 347, n. 6221, p. 536–539, 29 jan. 2015.

DISTRITO DE COLÚMBIA. *Civil Action 13-0851: Klayman, et. al. vs. Obama, et. al.* Disponível em: <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48>.

DISTRITO DE NOVA YORK. *Civil Action 13-3994: American Civil Liberties Union, et. al. vs. James R. Clapper, et. al.* Disponível em: <http://online.wsj.com/public/resources/documents/clapper.pdf>.

DONEDA, D. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

GALINDO AYUDA, F. Democracia, Internet Y Gobernanza: una Concreción. (Spanish). *Revista Seqüência.* v. 33, n. 65, p. 33–56, dez. 2012.

GARCÍA MARCO, F. J. Documentos juridicos y estandares tecnicos. In: GALINDO, F. (Ed.). **El** *derecho de la sociedad en red.* Zaragoza: Prensas de la Universidad de Zaragoza, 2013. p. 41–61.

GEERE, D. How deep packet inspection works. *Wired.* abr. 2012.

GELLMAN, B.; SOLTANI, A. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post.* 30 out. 2013.

GREENWALD, G. NSA collecting phone records of millions of Verizon customers daily. *The Guardian.* 6 jun. 2013.

GREENWALD, G.; KAZ, R.; CASADO, J. EUA espionaram milhões de e-mails e ligações de brasileiros - Jornal O Globo. *O Globo*. jul. 2013.

INTERNATIONAL TELECOMMUNICATION UNION. *Recommendation Y.2770 : Requirements for deep packet inspection in next generation networks*. Dubai: [s.n.]. Disponível em: <http://www.itu.int/rec/T-REC-Y.2770-201211-I/en>. Acesso em: 3 jan. 2015.

KEEN, A. The Cult of the Amateur: How blogs, MySpace, YouTube, and the rest of today's

user-generated media are destroying our economy, our culture, and our. *Random House LLC*, 2008.

_____. *Digital Vertigo: How Today's Online Social Revolution Is Dividing, Diminishing, and Disorienting Us.* London: Little, Brown Book Group, 2012.

KÜSTER, I.; HERNÁNDEZ, A. De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención de uso de las redes sociales en la web semántica. *Universia Business Review.* n. 37, p. 104–119, 2013.

LEMOS, R. 10 perguntas para Ronaldo Lemos, especialista em direito digital. *Istoé Dinheiro.* dez. 2012.

_____. O Marco Civil como simbolo do desejo por inovação no Brasil. In: LEITE, G.;

LEMOS, R. (Eds.). *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 03–11.

LESSIG, L. *Code.* 2. ed. New York: Basic Books, 2006.

MAHARREY, M. *California Lawmakers Introduce Fourth Amendment Protection Act, push back against NSA spying.* Disponível em: <http://www.offnow.org/california_lawmakers_introduce_fourth_amendment_protection_act_push_back_against_nsa_spying>. Acesso em: 10 jan. 2014.

MARTINELLI, G. N. S. F.; GOBI, G. O princípio da natureza participativa no Marco Civil da Internet: uma abordagem sobre a sua importância. In: LEITE, G. S.; LEMOS, R. (Eds.). *Marco Civil da Internet.* 1. ed. São Paulo: Atlas, 2014. p. 165–215.

MOLINARO, C. A.; SARLET, I. W. Breves notas acerca das relações entre a Sociedade em rede, a Internet e o assim chamado Estado de Vigilância. In: LEITE, G.; LEMOS, R. (Eds.). . *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 29–48.

MONTEIRO, M. *O Padrão Técnico de Inspeção Profunda de Pacotes de Rede | Observatório da Internet no Brasil.* Disponível em: <http://observatoriodainternet.br/o-padrao-tecnico-de-inspecao-profunda-de-pacotes-de-rede/>. Acesso em: 12 fev. 2013.

MORAES FILHO, J. F. Poder. In: BARRETTO, V. DE P. (Ed.). *Dicionário de filosofia do direito.* São Leopoldo: Unisinos, 2009. p. 640–642.

MORAIS, J. L. B.; NETO, E. J. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. In: LEITE, G.; LEMOS, R. (Eds.). *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 417–439.

OFF NOW. *Oklahoma state legislator introduces bill to banish NSA*. Disponível em: <http://www.offnow.org/oklahoma_state_legislator_introduces_bill_to_banish_nsa>. Acesso em: 10 jan. 2014.

OLIVEIRA, F. C. S.; OLIVEIRA, L. P. Abrindo, lendo e escrevendo as páginas do romance em cadeia: diálogos, backlash e hermenêutica. *Juris Poiesis.* v. 1, n. 14, p. 103–132, 2011.

PARISER, E. *O filtro invisível: O que a internet está escondendo de você.* 1. ed. Rio de Janeiro: Zahar, 2012.

POST, R.; SIEGEL, R. Roe Rage: Democratic Constitutionalism and Backlash. *Harvard Civil Rights-Civil Liberties Law Review.* v. 42, p. 373–433, 2007.

REFORM GOVERNMENT SURVEILLANCE. *Reform Government Surveillance.* Disponível em: <https://www.reformgovernmentsurveillance.com/>. Acesso em: 30 dez. 2013.

RUE, F. LA. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, publicada na décima sétima sessão do Conselho de Direitos Humanos da Assembleia Geral ocorrida em 16 de maio de 2011.* New York: [s.n.]. Disponível em: <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. Acesso em: 3 jan. 2015.

STECKLOW, S.; SONNE, P. Shunned Profiling Technology on the Verge of Comeback - WSJ. *The Wall Street Journal.* 24 nov. 2010.

STRECK, L. Apontamentos hermenêuticos sobre o Marco Civil regulatório da internet. In: LEITE, G. S.; LEMOS, R. (Eds.). *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 333–345.

TATLOW, D. K. Censored in China: “Today,” “Tonight” and “Big Yellow Duck” -

NYTimes.com. *The New York Times*. 4 jun. 2013.

VAIDHYANATHAN, S. *La googlización de todo.* Madrd: Océano, 2012.

Submissão: 30/09/2015
Aceito para Publicação: 06/12/2015