V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

ROSANE LEAL DA SILVA

MARCELO EDUARDO BAUZA REILLY

D598
Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UdelaR/Unisinos/ URI/UFSM /Univali/UPF/FURG;

Coordenadores: Marcelo Eduardo Bauza Reilly, Rosane Leal Da Silva – Florianópolis: CONPEDI, 2016.

Inclui bibliografia
ISBN: 978-85-5505-251-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Instituciones y desarrollo en la hora actual de América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Interncionais. 2. Direito. 3. Governança. 4. Novas tecnologias. I. Encontro Internacional do CONPEDI (5. : 2016 : Montevidéu, URU).

CDU: 34

Conselho Nacional de Pesquisa e Pós-Graduação em Direito
Florianópolis – Santa Catarina – Brasil
www.conpedi.org.br

Universidad de la República
Montevideo – Uruguay
www.fder.edu.uy

V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

Vive-se sob o impacto crescente do desenvolvimento tecnológico. Diariamente incontáveis produtos e serviços são projetados e disponibilizados no mercado global de consumo e a cada novo lançamento se renovam as promessas de mais qualidade de vida, redução de distâncias, maior conexão e felicidade.

A indústria desenvolvedora de tecnologia não mede esforços na criação de produtos e aplicativos mais dinâmicos e inteligentes e, amparados em poderosas campanhas de marketing, criam e/ou antecipam desejos de consumo. Novos lançamentos se sucedem num curto espaço de tempo, ditados mais pelo ritmo frenético da obsolescência programada do que por qualquer real necessidade dos usuários. No outro lado da cadeia de produção, consumidores ávidos por novidades não medem esforços para a aquisição de um novo dispositivo eletrônico e, cativados pelo discurso publicitário, apostam nas promessas mercadológicas como verdadeiras fórmulas garantidoras de uma vida plena e feliz.

Não é diferente no segmento das Tecnologias da Informação e Comunicação (TIC), cujos produtos, aplicativos e serviços seduzem milhares de usuários em todo o mundo. Em nenhum outro período histórico foi tão fácil e rápido obter informação e o acesso aos bens culturais como livros, músicas e filmes também experimentou relativa democratização.

Ao lado da pluralidade de fontes de consultas, a tecnologia alçou o consumidor, antes reduzido a um papel mais passivo, à condição de produtor de conteúdos, fato que se revela atrativo, especialmente para os internautas mais jovens, denominados nativos digitais. E as anunciadas vantagens não cessam no campo da informação, pois as experiências comunicativas também se renovam sob a promessa de conexão global.

Para permitir a comunicação instantânea e sem fronteiras são criados dispositivos móveis e variados aplicativos que tanto possibilitam contatos reservados entre um número limitado de atores, quanto interações mais amplas e públicas, ocorridas nos inúmeros sites de redes sociais. E o ato de comunicar ganha novos matizes, pois ao lado da palavra falada e escrita novos signos são incorporados, encontrando nas imagens e símbolos aliados para dar vazão à liberdade de expressão e comunicação.

Todas essas facilidades introduzem modos próprios de ser e estar no mundo, típicos da era digital, e incorporam ao vocabulário cotidiano verbos como “publicar”, “curtir” e “compartilhar”. Quando esses verbos se transformam em ações, experiências de vida tornam-se insumos de um mercado que não cessa de se expandir. Grande parte dessa expansão ocorre graças aos dados pessoais dos internautas, captados durante as interações on-line, momento em que os usuários das TIC abrem mão de sua privacidade em nome de experiências compartilhadas nos mais variados ambientes virtuais. Ao lado da disponibilização voluntária de informações também são utilizadas técnicas mais veladas de captura dos dados pessoais, tanto realizadas pelo mercado quanto pelos Estados.

Em grande medida essa foi a tônica das discussões que se realizaram no GT Direito, Governança e Novas Tecnologias, realizado no dia 09 de setembro de 2016, na Universidad de la República Oriental del Uruguay, em Montevidéu, aos auspícios do V Encontro Internacional do CONPEDI.

A seleção dos trabalhos que compõem a presente obra foi realizada após criteriosa avaliação (com dupla revisão cega por pares), o que resultou na qualidade dos dezesseis artigos apresentados nesta obra. Ainda que com enfoques distintos, os artigos guardam em comum a preocupação com os impactos produzidos pelo uso crescente das tecnologias da informação e comunicação, quer isso se revele como um desafio para a regulação da internet, nos efeitos que vai produzir na sua regulação, quer se manifeste nas relações entre os particulares.

Para dar maior coerência aos debates ao longo da apresentação, ocorrida no dia 09 de setembro de 2016, os trabalhos foram divididos em três eixos temáticos, assim distribuídos:

1) Temas mais gerais, que situam o leitor sobre os desafios impostos à sociedade e Estado em decorrência do uso das tecnologias da informação e comunicação, tanto pelo aspecto da governança, quanto em razão dos processos de regulação, o que pode ser encontrado nos artigos: A governança do endereçamento da rede: breve análise comparativa; A regulamentação da internet à luz da violação à liberdade de uso; Apartheid tecnológico ou tragédia dos comuns: a América Latina na sociedade da informação; Crimes de informática e cruzamento de informação a partir de dispositivos móveis; Os contratos eletrônicos e os deveres anexos: aspectos da boa-fé objetiva e as novas tecnologias.

2) Os potenciais das tecnologias da informação e comunicação como instrumento para atuação política, tema que foi objeto de atenção nos trabalhos: A influência das novas tecnologias no processo democrático; As novas tecnologias da informação e o e-gov como instrumento de participação social; Em tempos de comunicação digital a transparência e o

acesso à informação como condições indispensáveis para o exercício da cidadania democrática.

3) O terceiro eixo é composto por trabalhos que versam sobre novas formas de violação da privacidade e de dados pessoais, discutindo-se as estratégias para a sua proteção na sociedade em rede, temática que perpassa os trabalhos: A proteção de dados no e-processo: entre a publicidade do processo e a privacidade na era internet; A tutela da privacidade e a proteção à identidade pessoal no espaço virtual; A sociedade da informação como ambiente de transmissão de dados; Breves considerações sobre desafios à privacidade diante do big data na sociedade da informação; Os comunicadores instantâneos e o direito fundamental à privacidade nos ambientes corporativos; Privacidade e proteção de dados pessoais na era pós-Snowden: o Marco Civil da Internet mostra-se adequado e suficiente para proteger os internautas brasileiros em face da cibervigilância? Sociedade virtual do risco vs. Filosofia libertária criptoanarquista: livre manifestação do pensamento, anonimato e privacidade ou regulação, segurança e monitoramento da rede; Anotações sobre o marco civil da internet e o direito ao esquecimento.

Com nossos votos de boa leitura!

Profa. Dra. Rosane Leal da Silva - UFSM/Brasil

Prof. Dr. Marcelo Eduardo Bauzá Reilly - UDELAR/Uruguay

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA ERA PÓS-SNOWDEN: O MARCO CIVIL DA INTERNET MOSTRA-SE ADEQUADO E SUFICIENTE PARA PROTEGER OS INTERNAUTAS BRASILEIROS EM FACE DA CIBERVIGILÂNCIA?

PRIVACY AND PERSONAL DATA PROTECTION IN THE POST-SNOWDEN ERA: DOES INTERNET CIVIL MARK IS SHOWN ADEQUATE AND SUFFICIENT TO PROTECT BRAZILIAN INTERNET USERS IN FACE OF CYBER SURVEILLANCE?

Rafaela Bolson Dalla Favera [1]
Rosane Leal Da Silva [2]

Resumo

O objetivo deste artigo é discutir o direito à proteção da privacidade e dados pessoais no Brasil em face da vigilância realizada pelos Estados Unidos. Para tratar do tema parte-se das práticas de vigilância empreendidas pelo governo norte-americano, tanto aquelas denunciadas por Edward Snowden, quanto às realizadas posteriormente, objetivando-se discutir se a edição do Marco Civil da Internet consiste em resposta adequada e suficiente para tutelar os internautas brasileiros ante à vigilância na sociedade em rede. Concluiu-se pela insuficiência normativa e aponta-se para a necessidade de mobilização da academia com relação ao tema, cujo enfrentamento deve ser multissetorial.

Palavras-chave: Dados pessoais, Edward snowden, Marco civil da internet, Privacidade, Vigilância

Abstract/Resumen/Résumé

The purpose of this paper is to discuss the right of privacy protection and personal data in Brazil in face of surveillance conducted by United States. Addressing the issue, starts of the surveillance practices undertaken by north American government, both those reported by Edward Snowden, as that made later, aiming to discuss whether Internet Civil Mark edition consists in adequate and sufficient response to protect Brazilian internet users from surveillance in the network society. The conclusion was the regulatory failure and it has pointed out to the need to mobilize the academy on the issue, whose face should be multisectoral.

Keywords/Palabras-claves/Mots-clés: Personal data, Edward snowden, Internet civil mark, Privacy, Surveillance

---

[1] Mestranda do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (Linha de Pesquisa: Direitos na Sociedade em Rede) e integrante do Núcleo de Direito Informacional da instituição.

[2] Doutora em Direito pela UFSC. Professora do Curso de Graduação e Mestrado em Direito da Universidade Federal de Santa Maria. Coordena o Núcleo de Direito Informacional (UFSM).

INTRODUÇÃO

Espionagem e vigilância não são assuntos novos, muito pelo contrário, tais práticas sempre existiram, pois há relatos de sua ocorrência desde tempos mais remotos. O que efetivamente mudou, com o surgimento das Novas Tecnologias de Informação e Comunicação (TIC), em especial da *Internet*, foi o meio pelo qual tais práticas são desempenhadas. As novas tecnologias facilitam a espionagem e vigilância em massa que, na maioria das vezes, são praticadas por quem possui conhecimento técnico da arquitetura da rede, como os governos, as empresas, públicas ou privadas, e os *hackers* ou *crackers*.

No ano de 2013, Edward Snowden tornou público o monitoramento do governo norte-americano sobre as informações e dados de terceiros, em todo o mundo. A partir de então, esta temática passou a ser debatida com maior afinco pelos operadores do direito, tendo em vista violar o direito à privacidade e proteção de dados pessoais de pessoas localizadas em distintos países. Uma das medidas adotadas pelo governo brasileiro quanto ao ocorrido, foi apressar a publicação da Lei Nº 12.965/2014, ou Marco Civil da *Internet*, que, em certa medida, representou um avanço em termos normativos para o país, já que antes não contava com nenhuma legislação específica atinente à *Internet*.

Contudo, tendo em vista os movimentos nacionais e internacionais em defesa da proteção da privacidade e dados pessoais dos internautas, principalmente após as revelações de Snowden em 2013, pode-se dizer que os Estados Unidos se intimidaram com as repercussões do caso e contiveram suas ações de vigilância sobre outros países? Ademais, sob o prisma do Brasil, a edição do Marco Civil da *Internet* mostrou-se suficiente para barrar e/ou combater a *ciberespionagem* e a *cibervigilância* no país?

Para responder a essas indagações, o método de abordagem utilizado foi o dedutivo, partindo-se de uma análise doutrinária e legislativa da privacidade e dados pessoais, passando pelo estudo de um caso concreto, e finalizando com a verificação da efetividade da lei brasileira em resposta à espionagem e vigilância *cibernética* promovida por outros países, especialmente os Estados Unidos. Já o método de procedimento empregado foi o monográfico, apresentando-se um recente caso concreto no intuito de discutir se os Estados Unidos, passados três anos das manifestações do ex-técnico da *NSA*, continuam reiterando nas práticas de vigilância. O emprego desta metodologia importou na divisão do artigo em três seções.

1 DO NASCIMENTO DA *INTERNET* ATÉ A ERA PÓS-SNOWDEN: a crescente preocupação em torno da privacidade e dos dados pessoais dos internautas.

Dia após dia as Tecnologias de Informação e Comunicação (TIC) avançam, aprimorando-se. O episódio do surgimento da *Internet* no mundo interferiu significativamente na vida dos indivíduos, trazendo reflexos também sobre a forma de atuação das empresas e dos governos. Estes últimos se veem constantemente confrontados por novos desafios e demandas que decorrem da utilização dessas tecnologias, responsáveis, em parte, pela formação da sociedade em rede.

Manuel Castells (2013, p. 78), ao teorizar a respeito do poder na sociedade em rede, evidencia a presença de um novo Estado, um Estado em rede, o qual "[...] caracteriza-se por partilhar soberania e a responsabilidade entre diferentes Estados e níveis de governo [...]". Este Estado enfrenta um problema de coordenação, de níveis organizativo, técnico e político, um problema ideológico, e um problema geopolítico. O último relaciona-se à utilização, pelo governo global, de oportunidades em benefício de seus próprios interesses, sem, contudo, visar projetos comuns (CASTELLS, 2013, p. 79)[1].

Existem quatro formas, segundo Castells (2013, p. 80), de poder nas redes, quais sejam: poder de ligar-se em rede (*networking power*), poder da rede (*network power*), poder em rede (*networked power*), e poder para criar redes (*network-making power*) Mas o fato é que "O poder na sociedade em rede é o poder da comunicação." (CASTELLS, 2013, p. 93). Informação e comunicação não são a mesma coisa, pois enquanto a primeira é a mensagem transmitida, a segunda é a relação dessa mensagem (WOLTON, 2004, p. 24). Para Dominique Wolton a informação não cria comunicação, sendo essa o que realmente importa. O autor acredita que o ponto de partida do século XXI é a necessária ruptura e a difícil passagem da informação para a comunicação (WOLTON, 2004, p. 23).

No entanto, ainda que os usuários não façam esta distinção, é inconteste que a tecnologia tem sido cada vez mais utilizada para as atividades relacionadas à busca e publicação de informações, ao que se alia a comunicação, mantendo os indivíduos constantemente conectados. Toda essa interação origina intensos fluxos informacionais, o que desperta o interesse do mercado e dos governos, pois ninguém ignora que informação é poder.

Estes fluxos também geram desinformação, tal qual sustentado por Scott Lash (2005, p. 259-260), pois para ele, a desinformação é uma consequência imprevista da informação, em razão da sua sobrecarga, o que leva à impossibilidade de reflexão, à iracionalização e à falta de

[1] Para Castells (2013, p. 79) "[...] o mundo é *objectivamente multilateral*, mas alguns dos actores políticos mais poderosos no cenário internacional, como os EUA, Rússia ou China, *tendem a actuar unilateralmente, dando prioridade ao seu interesse nacional, sem se preocuparem pela desestabilização do mundo num sentido amplo*.".

inteligência. Além da possibilidade de supressão dos tempos e espaços necessários à reflexão sobre estes processos, o teor do conteúdo transmitido entre os usuários pode gerar vulnerabilidades, fragilizando a privacidade e a intimidade do internauta em face de terceiros.

Tais inquietações se intensificaram com as revelações de Edward Snowden em 2013, que desvendou o esquema de espionagem e vigilância promovido pela *National Security Agency* (*NSA*), a Agência de Segurança Nacional norte-americana[2].

Glenn Greenwald, no livro "Sem lugar para se esconder", elucida a trajetória do ex-técnico da *NSA* até o momento de sua denúncia, comprovada por inúmeros documentos obtidos da Agência, que revelaram que os Estados Unidos estavam obtendo todo o tipo de informações e dados[3] de pessoas físicas, jurídicas e até mesmo de outros governos, em todo o mundo (GREENWALD, 2014). Estas informações e dados eram adquiridos por intermédio de programas avançados e, muitas vezes, por meio da colaboração de provedores de *Internet*, a maioria deles, se não todos, sediados naquele país. Diante disso, e nas palavras de Greenwald (2014, p. 101) "[...] o governo dos Estados Unidos construía um sistema cujo objetivo é a completa eliminação da privacidade eletrônica no mundo inteiro."[4].

Como uma forma de justificar seus atos, o governo norte-americano informou estar priorizando a segurança nacional, principalmente com o intuito de evitar futuros ataques terroristas, já que desde 11 de Setembro o país passou a adotar medidas mais drásticas contra o terrorismo (GREENWALD, 2014, p. 212). Mas, tendo em vista os documentos divulgados por Snowden, comprovou-se que grande parte das informações e dados coletados não tinham ligação alguma com segurança nacional e terrorismo, tanto que os Estados Unidos não conseguiram evitar novos ataques desta natureza ocorridos após 11 de Setembro (GREENWALD, 2014, p. 214-215).

---

[2] Muito antes disso, Peréz Luño (2002, p. 108) expôs sua preocupação com a vigilância de outros Estados, dentre eles os Estados Unidos, através da Echelon e da Carnivore. Segundo o autor "Echelon y Carnivore son la muestra palpable de los riesgos que para la libertad de los ciudadanos implica la creación de sistemas de seguridad y control, no sometidos a controles por parte de instancias internacionales garantes de que la persecución de criminalidade en la Red, no pueda degenerar en una vigilancia incontrolada de millones de ciudadanos pertenecientes a todos los países del mundo. Los terribles e inexcusables atentados del 11 de Septiembre, no pueden servir de coartada para una limitación injustificable de los derechos y libertades cívicos.".

[3] O autor Danilo Doneda (2006, p. 152) diferencia "informação" de "dado", para ele a informação "[...] alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. [...] na informação já se pressupõe uma fase inicial de depuração de seu conteúdo [...]". Já o dado "[...] apresenta conotação um pouco mais primitiva e fragmentada, como observamos por exemplo em um autor que o entende como uma informação em estado potencial, antes de ser transmitida; o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração.".

[4] Edward Snowden não possuía nenhum motivo para se arriscar revelando ao mundo o que estava acontecendo, a não ser em razão da sua própria consciência, o que o fez afirmar "Eu não quero viver em um mundo onde não tenhamos privacidade nem liberdade, onde o valor único da internet seja destruído." (GREENWALD, 2014, p. 56).

Para David Lyon (2015, p. 9), a *surveillance* possui três dimensões, quais sejam: 1) Os governos dedicam-se à vigilância em massa de seus próprios cidadãos, mas as atividades da *NSA* repercutem em outros países também, não apenas nos Estados Unidos; 2) As corporações, especialmente as empresas de *Internet*, compartilham com os governos as suas próprias fontes de dados, em troca de alguns benefícios; 3) Os cidadãos comuns também participam através das suas interações *online*, especialmente por meio das redes sociais e do uso de celulares. São esses três elementos que facilitam a vigilância e, consequentemente, a violação da privacidade e dados pessoais.

Por outro lado, Bauman (2013, p. 20), ao teorizar a respeito da vigilância líquida[5], entende que o anonimato, a confidencialidade e a privacidade são questões importantes, mas não as de maior relevância, pois a imparcialidade, a justiça, as liberdades civis e os direitos humanos também devem ser levados em consideração. Isso porque, para ele, "[...] a *categorização social* é basicamente o que a vigilância realiza hoje, para o bem ou para o mal.". Castells (2007, p. 219) acredita que a vigilância e as violações acontecem porque não existe uma relação de confiança mútua entre os governos e os seus cidadãos, além de os primeiros não serem aliados da liberdade. Para o referido autor (CASTELLS, 2007, p.220),

> [...] a Internet bem poderia servir para que os cidadãos vigiassem o seu governo e não para que o governo vigiasse os seus cidadãos. Poderia transformar-se num instrumento de controlo, informação, participação e mesmo de tomada de decisões estruturado de baixo para cima. Os cidadãos poderiam ter acesso aos arquivos do governo, o que constitui de facto um direito seu. Teriam que ser os governos e não as vidas privadas das pessoas a transformar-se em casas de cristal, à exceção de algumas questões fundamentais de segurança nacional.

No entanto, ao contrário do sustentado pelo doutrinador, é a vida das pessoas comuns que se transforma numa "casa de cristal". Lyon (2015, p. 101), questiona se atualmente a privacidade ainda seria um valor e responde afirmativamente ao associá-la às políticas públicas[6]. Explica que o próprio contexto faz a diferença para compreender o que é "privacidade", especialmente nas comunicações *online*, e que as políticas de privacidade estão

[5] Para Bauman (2013, p. 10), "Vigilância líquida" é menos uma forma completa de especificar a vigilância e mais uma orientação, um modo de situar as mudanças nessa área na modernidade fluida e perturbadora da atualidade. A vigilância suaviza-se especialmente no reino do consumo. Velhas amarras se afrouxam à medida que fragmentos de dados pessoais obtidos para um objetivo são facilmente usados com outro fim. A vigilância se espalha de formas até então inimagináveis, reagindo à liquidez e reproduzindo-a. Sem um contêiner fixo, mas sacudida pelas demandas de "segurança" e aconselhada pelo marketing insistente das empresas de tecnologia, a segurança se esparrama por toda parte.".

[6] Como política pública, ou seja, como questão de importância pública, a privacidade é frequentemente expressa em termos de benefícios sociais e societais, em ambos os lados do Atlântico e além (LYON, 2015, p. 99-100).

sendo constantemente desenvolvidas para tentar garantir que elas permanecem relevantes (LYON, 2015, p. 99-100).

Bauman (2013, p. 44), por sua vez, compreende que "No final, a escolha é entre segurança e liberdade: você precisa de ambas, mas não pode ter uma sem sacrificar pelo menos parte da outra; e quanto mais tiver de uma, menos terá da outra." De fato, o tema é controverso, o que revela a importância de se observar as principais previsões normativas que abarcam o direito à privacidade no ordenamento jurídico brasileiro.

A mais importante, por considerar a privacidade um direito fundamental, é a Constituição Federal de 1988, em seu artigo 5º, inciso X. Embora a palavra "privacidade" não conste expressamente no texto legal, os constitucionalistas entendem pela sua incorporação. Mesmo que alguns autores, como afirmam Mendes e Branco (2015, p. 280), considerem haver distinções entre privacidade, intimidade e vida privada[7], no presente trabalho a privacidade é empregada como um conceito amplo, que abarca os demais, tendo em vista as habilidades do governo norte-americano em obter todo o tipo de informações e dados de terceiros[8].

Quanto à teoria dos direitos fundamentais, faz-se importante referir as cinco gerações (ou dimensões) de direitos evidenciadas por Bonavides, muito embora essa classificação varie de autor para autor. A primeira geração compreende os direitos de liberdade e pressupõe uma atuação negativa do Estado. A segunda, os direitos de igualdade, e requer uma atuação positiva do Estado. A terceira geração compreende os direitos de fraternidade, que focalizam o gênero humano, enquanto a quarta destaca os direitos de globalização política. E, por fim, a quinta geração de direitos, coloca em relevo o direito à paz (BONAVIDES, 2011).

O direito à privacidade relaciona-se aos direitos civis e políticos o que, pela teoria tradicional, geraria uma abstenção do Estado, ou seja, sua satisfação seria decorrência da não intervenção indevida na esfera privada de outrem. No entanto, esta tradicional teoria da geração de direitos cedeu espaço para construções mais atuais, que defendem as dimensões de direitos, posição segundo a qual além de não haver a substituição de uma geração por outra em decorrência da complementaridade dos direitos, ainda se propagou a compreensão de que o

[7] Conforme Mendes e Branco (2015, p. 280), há quem entenda que "O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas." Para eles, "[...] a expressão "vida privada" cobre um vasto campo e está sujeita a interferências emocionais." (MENDES; BRANCO, 2015, p. 281).

[8] Peréz Luño, na obra "Los derechos humanos en la sociedad tecnológica", evidencia a superação dessas divisões na era tecnológica (2005).

respeito à privacidade também exige atividades positivas por parte do Estado, que tem o dever de garantir a autonomia informacional aos cidadãos.

Destaque-se que aliado à previsão constitucional também existe proteção infraconstitucional, já que o tema é tratado como direitos da personalidade. Nesse sentido, a partir de Canotilho (2003, p. 296) pode-se dizer que "Muitos dos direitos fundamentais são direitos de personalidade, mas nem todos os direitos fundamentais são direitos de personalidade." Para o doutrinador, os direitos de personalidade englobam os direitos de Estado, os direitos sobre a própria pessoa, os direitos distintivos da personalidade e muitos dos direitos de liberdade. Mas, atualmente, "[...] cada vez mais os direitos fundamentais tendem a ser direitos de personalidade e vice-versa.".

Assim, a privacidade, apesar de ser compreendida como um direito fundamental, também é um direito da personalidade, especialmente por figurar no artigo 21 do Código Civil de 2002. Todavia, autores como Anderson Schreiber (2011, p. 128) dizem que o atual Código Civil deu à privacidade um tratamento inadequado, já que lhe dedicou um único artigo que possui enunciado genérico. Conforme o autor, "Perdeu, assim, a oportunidade de oferecer parâmetros para a solução de diversos conflitos concretos ligados à tutela da privacidade.".

No âmbito internacional, pode-se dizer que a principal previsão contendo o direito à privacidade para além das fronteiras dos Estados, é a Declaração Universal dos Direitos Humanos de 1948, que contempla o tema em seu artigo XII.

A existência de previsão normativa nacional e internacional permite constatar que o problema envolvendo o direito à privacidade atualmente não se liga a sua positivação, mas sim a sua efetividade. Fato que suscita atenção dos autores é que nestes documentos não estaria prevista expressamente a proteção de dados pessoais, discutindo-se se estão albergados no direito à privacidade ou se constituiriam nova categoria.

Marcel Leonardi (2011, p. 67-68) expõe a opinião de alguns autores para os quais o direito à proteção de dados pessoais estaria envolto no direito à privacidade. Nesse sentido, "O atributo básico do direito à privacidade seria, portanto, a capacidade de o indivíduo controlar a circulação de informações a seu respeito." Contudo, Leonardi (2011, p. 78) discorda dessa corrente, pois, segundo ele,

> [...] conceituar privacidade *apenas* como o controle sobre informações e dados pessoais pode ser, ao mesmo tempo, muito abrangente, na ausência de uma definição para "controle" e de delimitação de quais dados devem ser protegidos, ou muito restritivo, em razão de reduzir a privacidade a aspectos relacionados apenas a informações e de enfatizar a autonomia da vontade do indivíduo.

Danilo Doneda (2006, p. 151), por seu turno, sustenta que "O discurso sobre a privacidade cada vez mais concentra-se em questões relacionadas a dados pessoais e, portanto, informação." Este autor insiste na observância de cinco princípios fundamentais, quais sejam: 1) Princípio da publicidade (ou da transparência), que requer o conhecimento público dos bancos de dados que contenham dados pessoais; 2) Princípio da exatidão, no sentido da necessidade de os dados coletados representarem fielmente a realidade; 3) Princípio da finalidade, em que antes da coleta dos dados pessoais, deve haver a comunicação da sua finalidade ao interessado; 4) Princípio do livre acesso, cujo objetivo é possibilitar aos indivíduos o acesso aos bancos de dados onde se encontram informações a seu respeito; 5) Princípio da segurança física e lógica, no intuito de proteger os dados "[...] contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado." (DONEDA, 2006, p. 216-217).

Para Schreiber (2011, p. 151), o princípio da finalidade, que ele denomina de "princípio da especificação dos propósitos", é de extrema relevância, pois o titular dos dados pessoais tem o direito de ser informado quanto ao propósito da coleta, sendo que os dados só podem ser utilizados para a finalidade declarada. O autor ainda salienta a relação direta desse princípio com o da boa-fé objetiva no direito civil. Disso constata-se que a *NSA*, ao promover a espionagem e a vigilância em massa revelada por Snowden em 2013, violou todos esses princípios referentes aos dados pessoais, além, é claro, de ferir gravemente a privacidade de terceiros. Este acontecimento fez aumentar as preocupações em torno da privacidade e dados pessoais em todo o mundo, sendo que no Brasil uma das atitudes relevantes em resposta a essa prática foi a promulgação da Lei Nº 12.965/2014 (Marco Civil da *Internet*), que será estudada na terceira seção deste trabalho.

Seguindo essa lógica, Pilati e Olivo (2014, p. 293) lançam um novo olhar sobre o direito à privacidade, um olhar "coletivo". Para eles,

> Com a presença constante e invasiva, e cada vez mais democrática, de novas tecnologias, os valores relacionados à privacidade, como vem sendo demonstrado, acabam por sofrer uma forte readequação conceitual. Dessa forma, permite-se, aqui, ir além da teorização moderna, que não possibilita classificações fora das molduras pública e privada, e analisar a privacidade sob um novo prisma: como um bem Coletivo, ou seja, um bem que se situa na esfera de titularidade da Sociedade, e não apenas do indivíduo. [...] A questão, então, ganha ainda mais amplitude, pois se constata que não apenas o indivíduo pode sofrer violação desse bem; transfere-se o problema para além da perspectiva meramente individual e passa-se a analisar a privacidade da Sociedade, enquanto sujeito de direitos coletivos.

Este novo olhar, de importância ímpar no cenário atual, já havia sido teorizado por Stefano Rodotà (2008, p. 30) ao afirmar que "[...] a invocação de privacidade supera o tradicional quadro individualista e dilata-se em uma dimensão coletiva, tendo em vista que não se leva em consideração o interesse do indivíduo enquanto tal, mas como pertencente a um determinado grupo social.". No mesmo sentido segue Helen Nissenbaum (2011, p. 95) ao enfatizar o valor da privacidade para a sociedade, destacando seu aspecto comum, público e coletivo. Sustenta que o fracasso das leis e regras "[...] son resultado de asociar la privacidad con los intereses de las personas, los que al final suelen verse opacados por necesidades sociales antagónicas, extremas o no [...]".

Tal constatação reforça o direito à privacidade e, também, à proteção de dados pessoais, visto que frente aos acontecimentos recentes, especialmente da *ciberespionagem* e *cibervigilância* norte-americana, há que se buscar, mediante a coletividade, uma maior proteção, já que os indivíduos, enquanto grupo social, possuem uma maior força de reversão desse quadro, do que isoladamente.

Diante do que foi exposto na primeira seção deste trabalho e, tendo em vista as graves violações cometidas pela Agência de Segurança Nacional dos Estados Unidos, seguido de pronunciamentos e atos em oposição à espionagem e à vigilância em massa em todo o mundo, especialmente no Brasil, a seguir procurar-se-á evidenciar, por intermédio de um recente caso concreto, que o governo norte-americano não se intimidou com tudo o que sucedeu às revelações de Snowden, e continua violando a privacidade e os dados pessoais de terceiros.

2 A VIGILÂNCIA GOVERNAMENTAL NORTE-AMERICANA PERSISTE? O recente caso *Microsoft Corporation* v. *The United States Department of Justice* e Loretta Lynch.

Após Edward Snowden confessar ao mundo o que, para grande parte dos indivíduos estava oculto, ao menos em tamanhas proporções, pensou-se, erroneamente, que o governo dos Estados Unidos iria pôr fim ao que vinha realizando de forma indiscriminada. Contudo, um recente caso, que será exposto a partir de agora, revela que aquele país continua espionando e vigiando internautas em toda a rede, mesmo passados três anos das revelações que o colocaram no topo das preocupações, principalmente, da mídia e dos operadores do direito.

Trata-se de uma ação ajuizada em abril de 2016 na cidade de Seattle, em Washington, pela *Microsoft Corporation* contra o Departamento de Justiça dos Estados Unidos e Loretta Lynch, na qualidade de procuradora geral daquele país. De acordo com a petição inicial

disponibilizada na *Internet*, a *Microsoft* ingressou com a demanda visando ao direito de informar aos seus usuários do serviço de computação em nuvem que o governo norte-americano estava colhendo informações e dados a respeito deles (EUA, 2016).

A autora da ação enfatiza o direito dos usuários de serem informados, e o dever da empresa de cientificá-los, quando o governo obtém uma autorização para explorar informações e dados na nuvem. O réu, amparado pela *section* 2705 (b) do *Electronic Communications Privacy Act* de 1986, "[...] allows courts to order Microsoft to keep its customers in the dark when the government seeks their email content or other private information, based solely on a "reason to believe" that disclosure might hinder an investigation."[9] (EUA, 2016). Para a *Microsoft*, a *section* 2705 (b) desta lei viola tanto a Primeira Emenda quanto a Quarta Emenda da Constituição dos Estados Unidos, e deve ser declarada inconstitucional.

Quanto ao tema, Helen Nissenbaum (2011, p. 101-102) destaca que,

> En Estados Unidos, la Constitución es una fuente de protección legal contra la intromisión del gobierno. Este documento, cuyos autores recibieron la influencia del derecho consuetudinario inglés y el canon histórico de la filosofía política que ha inspirado a democracias del mundo entero, expone principios fundamentales que definen y limitan las facultades del gobierno. Algunos de los más importantes derechos y libertades para los particulares em relación con el gobierno se desarrollan em la serie de enmiendas constitucionales que componen la Carta de Derechos. Pese a que en ella no aparece nunca en forma explícita el término privacidad, la protección de ésta está incorporada en varias de sus enmiendas.

A Primeira Emenda prevê, basicamente, que o Congresso não poderá legislar estabelecendo uma religião, ou proibindo o livre exercício dos cultos. E que também não cerceará a liberdade da palavra, de imprensa, o direito das pessoas de se reunirem pacificamente, e de peticionarem ao governo para a reparação de seus agravos[10]. Para a autora da ação isso significa a consagração do direito da empresa de falar aos seus usuários, e de discutir como o governo conduz as suas investigações (EUA, 2016).

Já a Quarta Emenda designa o direito do ser humano de não ser infringido quanto à inviolabilidade do próprio indivíduo, das casas, dos papéis e dos haveres, contra buscas e apreensões arbitrárias. Além de nenhum mandado poder ser expedido, a não ser mediante a confirmação de indícios de culpabilidade, por juramento ou declaração, devendo também haver

[9] "[...] permite aos tribunais ordenarem a Microsoft a manter seus clientes no escuro quando o governo procura o conteúdo de seus e-mails ou outra informação privada, baseados unicamente em uma "razão para acreditar" que a divulgação poderia limitar uma investigação." (Livre tradução)

[10] "Amendment I (1791) Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (EUA).

a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas[11]. Para a *Microsoft* isso permite que os indivíduos e as empresas tenham a prerrogativa de saber se o governo busca ou apreende seus bens (EUA, 2016).

O fato é que "People do not give up their rights when they move their private information from physical storage to the cloud."[12] (EUA, 2016). Resumidamente, a computação em nuvem, ou *cloud computing*, "[...] é uma ideia que nos permite utilizar as mais variadas aplicações via internet, em qualquer lugar e independente da plataforma, com a mesma facilidade de tê-las instaladas em nosso próprio computador [...]" (VELTE A.; VELTE T.; ELSENPETER, 2012, p. 4).

Os serviços de computação em nuvem, que já não são mais novidade, facilitam a interação de pessoas físicas e jurídicas com suas informações e dados lá colocados, pela *Internet*. No momento em que um determinado arquivo encontra-se na nuvem, o seu titular pode acessá-lo por meio de qualquer dispositivo, seja um computador, *notebook*, *tablet*, celular etc., desde que conectado à rede mundial de computadores. Além de acessá-lo, o titular também tem a possibilidade de editá-lo, dispensando, por exemplo, o uso de HDs externos ou *pen drives* (VELTE A.; VELTE T.; ELSENPETER, 2012). Nos tempos atuais essas facilidades revelam-se muito úteis.

Os autores Anthony, Toby e Robert (2012, p. 22) consideram a *Microsoft* como uma das precursoras e, hoje, uma das "titãs" da computação em nuvem. Mesmo assim, para eles, "A Microsoft está um pouco atrasada para a festa na nuvem e não é líder em computação em nuvem. Esta honra vai para o Google e Amazon, entre outras empresas que oferecem serviços de computação em nuvem [...]". Ainda, quanto à segurança, os mesmos autores advertem que "Tal como um ponto de partida, admita que qualquer coisa que você colocar numa nuvem pode ser acessada por qualquer um." (ANTHONY, TOBY, ROBERT, 2012, p.35). Conclui-se, assim, que a nuvem não é segura, e que a única forma de ninguém ter acesso às informações e dados de terceiros é eles não estando lá alojados.

Na ação judicial em apreço, a autora revela que entre setembro de 2014 e março de 2016 a *Microsoft* recebeu cinco mil seiscentas e vinte e quatro exigências federais para a obtenção de acesso à informações ou dados de usuários. Dessas, duas mil quinhentas e setenta e seis,

[11] "Amendment IV (1791) The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (EUA).

[12] "As pessoas não desistem dos seus direitos quando elas movem as suas informações privadas do armazenamento físico para a nuvem." (Livre tradução)

quase metade, vieram acompanhadas de ordens de sigilo, proibindo a empresa de informar os seus clientes a respeito da vigilância governamental. Além disso, mil setecentas e cinquenta e duas dessas ordens de sigilo não continham limitação de tempo, o que significa que a empresa poderia ser proibida indeterminadamente de comunicar aos consumidores do serviço de computação em nuvem afetados sobre as intrusões do governo (EUA, 2016).

Embora considerando que este processo esteja em curso nos Estados Unidos, e mesmo que a autora da ação não tenha feito referência na petição inicial, interessa questionar se o governo norte-americano, por intermédio da *section* 2705 (b) do *Electronic Communications Privacy Act* de 1986, possui permissão para acessar indiscriminadamente informações e dados de usuários da *Microsoft* de outros países, como o Brasil. Essa preocupação faz sentido porque a empresa está sediada nos Estados Unidos, mas possui inúmeras filiais e escritórios ao redor do mundo, inclusive no Brasil.

Há pouco tempo André Dantas expôs suas inquietações nesse sentido, afirmando que os norte-americanos tendem a pressionar, de inúmeras formas, os demais países para a implementação de suas normas, ainda que contra o interesse deles ou de forma silenciosa. Ele também enfatiza que "A constante disputa entre a evolução técnica dos computadores e as legislações cada vez mais restritivas podem levar a uma sociedade totalmente intolerante." (DANTAS, 2016).

Diante do presente caso, o qual está em fase inicial, é possível perceber que mesmo por meio de brechas normativas o governo norte-americano continua espionando e vigiando informações e dados de terceiros, não só dos Estados Unidos, mas muito provavelmente de cidadãos de outros países. O que Snowden relatou em 2013, portanto, não foi suficientemente grave para intimidar essas práticas por parte do governo norte-americano. A constatação pública e mundial sobre a *ciberespionagem* e *cibervigilância* exige a tomada de atitude por parte dos demais países, seja por meio da implementação de novas leis, seja através do aperfeiçoamento das TIC, a fim de rechaçar tais violações à privacidade e aos dados pessoais.

No Brasil, a Lei Nº 12.965/2014, conhecida também como Marco Civil da *Internet*, entrou em vigor logo após as revelações do ex-técnico da *NSA* e consistiu numa resposta do governo brasileiro às violações dos fluxos informacionais. Na terceira e última seção deste trabalho, esta norma será estudada e serão analisadas suas potencialidades para barrar e/ou combater a espionagem e a vigilância governamental daquele país. A intenção é demonstrar que o Marco Civil é necessário e adequado para os brasileiros, pois inovador, mas não suficiente contra a vigilância mais incisiva que é realizada pelos Estados Unidos, como a seguir será evidenciado.

3 O MARCO CIVIL DA *INTERNET* NO BRASIL: necessário mas não suficiente para barrar e/ou combater a vigilância.

A Lei Nº 12.965/2014, também denominada Marco Civil da *Internet*, "[...] é um dos principais exemplos globais de lei redigida por meio de procedimentos abertos e colaborativos." (LEMOS, 2015, p. 82). Em um primeiro momento, o Projeto de Lei Nº 84/1999, popularmente conhecido como "Lei Azeredo", previa uma regulamentação criminal para o uso da *Internet* no Brasil. Diante disso, Ronaldo Lemos, Carlos Affonso Pereira de Souza e Sergio Branco propuseram um projeto alternativo àquele, e ressaltaram a importância da existência de uma regulamentação civil e não criminal, que contemplasse direitos fundamentais na rede. Isso porque o direito criminal só pode ser empregado como *ultima ratio* e, sendo assim, o Marco Civil foi indicado como o caminho mais adequado a ser perseguido (LEMOS, 2015, p. 83).

Dentre as trocas de e-mails daqueles envolvidos no projeto e o governo brasileiro, Ronaldo Lemos destaca que "A mensagem clara ali era de que a estrutura e a proposta concretas do Marco Civil não viriam do governo. Caberia diretamente à sociedade civil realizar a arquitetura do projeto." (2015, p. 92). E foi justamente esse caráter não governamental e colaborativo que tornou a lei inovadora e um modelo multissetorial promissor de relação entre direito e tecnologia, inclusive para outros países (LEMOS, 2015, p. 100).

A lei, que estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no país, possui em suas disposições preliminares oito princípios norteadores. Para De Lucca (2015, p. 45), "[...] tudo o que existe no mundo jurídico – sejam *princípios*, sejam simplesmente *regras* – constituem, em última análise, *normas*." Dentre os princípios do artigo 3º, encontram-se o da proteção da privacidade, no inciso II, e o da proteção dos dados pessoais, na forma da lei, no inciso III. Como já visto, ainda não existe uma legislação que regulamente a proteção de dados pessoais no Brasil, mas alguns autores compreendem que o não cumprimento de um princípio, aqui entendido como norma, é a forma mais grave de inconstitucionalidade ou ilegalidade (DE LUCCA, 2015, p. 50).

Na sequência, o artigo 7º, inserido no capítulo dos direitos e garantias dos usuários, sofreu, de acordo com Lima e Bioni (2015, p. 265), acréscimos em seus incisos após o caso Snowden, já que antes possuía cinco previsões e após o ocorrido passou a contar com oito incisos. Os autores (2015, p. 266) salientam dois deles, quais sejam os incisos VIII e IX. Frente a isso, eles também expõem duas teorias aplicáveis, a da *Human Computer Interaction* e a da *Privacy by Default*. A primeira supõe uma maior interação entre o homem e o computador, já

que leva em consideração a capacidade cognitiva do usuário de reagir ao que acontece na rede. Para tanto, é necessário um processo de comunicação no qual o usuário é informado a respeito da possibilidade de gerir os seus dados pessoais (LIMA; BIONI, 2015, p. 271-272).

A *Privacy by Default*, por sua vez, que nasce da *Privacy by Design*, parte do pressuposto de que o direito e a tecnologia se intercruzam. Disso almeja-se que o próprio produto ou serviço, como os provedores de *Internet*, seja arquitetado com a finalidade de proteger as informações pessoais dos seus usuários (LIMA; BIONI, 2015, p. 277). Conforme tais autores (2015, p. 278), "Tal conceito impõe que o próprio sistema de informação (arquitetura da rede) garanta um ambiente seguro para a coleta, tratamento e transferência de dados, sempre informando o titular destes que pode configurar a ferramenta tecnológica como lhe aprouver.". Essa autodeterminação informacional e a adjetivação do consentimento, compreendidas pelas duas teorias, é o que em parte a *Microsoft* quer implementar no caso apresentado na segunda seção deste trabalho.

Muito embora haja um capítulo, no Marco Civil da *Internet*, que englobe a proteção de dados pessoais (capítulo III, seção II), esse não contempla as medidas que serão utilizadas diante da verificação da espionagem e vigilância, especialmente de outros países, ou as formas de barrar e/ou combater tais práticas. É por essa, e outras razões, que autores como Meyer-Pflug e Leite (2015, p. 444) sustentam que "A legislação doméstica por si só não dá conta das inúmeras violações de direitos presentes na rede mundial de computadores. Dentro desse contexto, esse tema merecerá um tratamento mais específico no plano internacional, de modo a incluir a agenda de direitos humanos.".

De acordo com Barbosa (2015, p. 249), a própria redação do Marco Civil possui como consequência inequívoca o estado de vigilância. Sendo assim, a lei não resolve o problema da *ciberespionagem* e *cibervigilância* dos Estados Unidos. E, conforme o autor, "As multinacionais, que prestam serviços on-line, certamente não vão deixar de colaborar com o governo norte-americano vigiando os internautas devido à lei do Brasil.".

Nesse contexto, mister referir os treze princípios internacionais sobre a aplicação de direitos humanos à vigilância das comunicações, são eles: 1) Legalidade: os limites do direito à privacidade precisam estar definidos em lei e serem revistos regularmente; 2) Fim legítimo: a vigilância das comunicações só pode ser empregada para conquistar os objetivos mais relevantes do país; 3) Necessidade: é preciso comprovar a necessidade da vigilância; 4) Adequação: a vigilância das comunicações deve alcançar, de forma efetiva, o seu fim; 5) Proporcionalidade: a vigilância deve se pautar pela proporcionalidade e autorização judicial competente e prévia; 6) Autoridade judicial competente: deve ser imparcial e independente; 7)

Devido processo legal: requer o procedimento judicial, em audiência pública e justa, em matéria de direitos humanos; 8) Notificação do usuário: realizar a notificação prévia dos indivíduos quanto à decisão de vigilância das comunicações; 9) Transparência: o governo deve publicizar o escopo e a natureza das suas atividades desse tipo; 10) Escrutínio público: necessidade da criação de mecanismos de fiscalização; 11) Integridade das comunicações e sistemas: os demais atores não podem ser compelidos pelo Estado a praticarem vigilância; 12) Salvaguardas para a cooperação internacional: pressupõe a assistência de provedores estrangeiros na vigilância governamental, regulado por tratados claros e públicos; 13) Salvaguardas contra o acesso ilegítimo: necessidade de implementação de penalidades, na esfera civil e penal, frente à vigilância ilegal (ANTONIALLI; ABREU, 2015, p. 37-38).

A *Article* 19, uma organização que defende a liberdade de expressão e informação, apresentou um estudo no qual concluiu que o Brasil está muito distante de efetivar esses princípios na prática. A pesquisa também constatou que "[...] as respostas às denúncias de Edward Snowden pouco adiantaram para alertar o poder público a respeito da segurança cibernética [...]", isso porque o Brasil não se ateve à *cibersegurança*, mas sim à *ciberguerra* (ARTICLE 19, p. 44).

Nesta pesquisa foi demonstrado que o país investiu em respostas militares e adotou a doutrina da guerra *cibernética*[13] (ARTICLE 19, p. 44). Isso fez com que aumentasse o "[...] monitoramento de comunicações sem a transparência que se espera em uma sociedade democrática.". Assim, a principal preocupação quanto à implementação dessas políticas é a de que o Brasil cometa os mesmos erros que os Estados Unidos, e acabe por violar a privacidade e dados pessoais de terceiros (ARTICLE 19, p. 46). Além disso, para esta organização em específico, "Não há um alinhamento ou mesmo interesse em acabar ou evitar que a vigilância em massa seja possível no país, pois não é politicamente unânime que a sua existência seja nociva para o desenvolvimento da humanidade." (ARTICLE 19, p. 45).

Ocorre que, no dia onze de maio de 2016, foi publicado o Decreto Nº 8.771/2016 que regulamenta algumas questões do Marco Civil da *Internet*. Uma delas se refere ao conceito de "dado pessoal" que significa "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016).

[13] Conforme a *Article* 19, *ciberguerra* ou guerra *cibernética* "[...] pode ser compreendida, de maneira geral, como um confronto via meios eletrônicos e informáticos – via internet – e que costumam ter como alvo infraestruturas críticas, notadamente bens de interesse público como redes de energia elétrica, de gás e de água, os serviços de transportes, os serviços de saúde e financeiros.". Já o termo *cibersegurança* ou segurança *cibernética* "[...] pode ser definida como a proteção de sistemas, redes e dados no ciberespaço." (ARTICLE 19, p. 9).

Tal Decreto também prevê, em seu artigo 11 e parágrafo 3º, que as autoridades administrativas, que visam o acesso à dados cadastrais[14], devem estar amparadas por um fundamento legal de competência expressa e de motivação para o pedido de acesso. Além da necessidade desse pedido "[...] especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos." (BRASIL, 2016).

Também são estipuladas, para os provedores de conexão e aplicações de *Internet*, diretrizes sobre padrões de segurança, as quais estão inseridas no artigo 13, tais como: 1) Estabelecimento de controle estrito sobre o acesso aos dados através da definição de responsabilidades daqueles que terão o acesso permitido; 2) Previsão de mecanismos de autenticação de acesso aos registros; 3) Criação de inventário detalhado dos acessos aos registros, como o momento, a duração, o arquivo acessado etc.; 4) Uso de soluções de gestão dos registros que visem garantir a inviolabilidade dos dados (BRASIL, 2016).

Estas regulamentações, e as demais contidas no Decreto, são relevantes, principalmente por abarcarem alguns dos princípios internacionais sobre a aplicação de direitos humanos à vigilância das comunicações, mencionados anteriormente. Todavia, ainda deve-se avançar muito, em todos os sentidos, para alcançar uma efetiva proteção da privacidade e dados pessoais de terceiros na *Internet*, além de encontrar um meio capaz de barrar e/ou combater a espionagem e vigilância de outros países, sem ferir direitos fundamentais e da personalidade.

Por fim, cumpre referir o posicionamento de Kevin D. Haggerty (2015, p. 227) quanto aos assuntos versados no presente trabalho. Para ele, a infraestrutura da privacidade não tem sido particularmente bem sucedida, a longo prazo, na redução da expansão da vigilância. Ademais, os regulamentos justificados como uma maneira de proteger a privacidade podem ajudar a expandir a vigilância. Sustenta que os desenvolvimentos no capitalismo de informações ameaçam reconfigurar drasticamente, ou mesmo oprimir, a proteção da privacidade nos próximos anos. Nas palavras do autor, "The decline of privacy is all around us, but it is paradoxically hard to see."[15] (HAGGERTY, 2015, p. 227).

Haggerty (2015, p.231) também salienta que,

> The contemporary expansion of surveillance, where monitoring becomes an ever-more routine part of our lives, represents a tremendous shift in the balance of power

[14] Diferentemente dos dados pessoais, os "dados cadastrais" englobam, conforme o Decreto, a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário (BRASIL, 2016).
[15] "O declínio da privacidade está ao nosso redor, mas é paradoxalmente difícil ver." (Livre tradução)

> between citizens and organizations. Perhaps the greatest danger of this situation is how our existing surveillance practices can be turned to oppressive uses.[16]

Ao final, o autor não oferece uma alternativa de enfrentamento ao problema sob o argumento de que quando cientistas, médicos ou os engenheiros identificam um problema, não se espera necessariamente que eles forneçam uma solução (HAGGERTY, 2015, p. 232). Realmente, pensar em uma solução eficaz e a curto prazo para resolver o problema da *ciberespionagem* e da *cibervigilância* governamental norte-americana, é um desafio, mas que precisa começar a ser refletido para que no futuro a privacidade e os dados pessoais de terceiros sejam, de fato, protegidos, especialmente por dizerem respeito a questões atinentes aos direitos humanos.

CONCLUSÃO

Diante de tudo o que foi apresentado neste trabalho, algumas conclusões podem ser extraídas. Há que se ter em mente que um longo caminho foi percorrido desde o nascimento da *Internet* até a era pós-Snowden, mas não maior do que aquele entre o surgimento da espionagem e vigilância no mundo e os tempos modernos. Tais práticas sempre existiram, contudo foi com o auxílio das novas Tecnologias de Informação e Comunicação (TIC) que se intensificaram e se tornaram massivas.

Desde as revelações de Edward Snowden em 2013, a respeito do monitoramento indiscriminado de informações e dados de terceiros, pessoas físicas, jurídicas ou outros governos, nacionais ou estrangeiros, pelos Estado Unidos, ganharam destaque as teorizações a respeito da proteção do direito à privacidade e dados pessoais. No Brasil, o direito à privacidade encontra previsão normativa na Constituição Federal de 1988, no Código Civil de 2002, e no Marco Civil da *Internet* de 2014. Já no plano internacional, este direito é abarcado pela Declaração Universal dos Direitos Humanos de 1945, dentre outras.

O direito à proteção de dados pessoais, por sua vez, é genericamente tutelado pelas legislações brasileiras, no entanto, recentemente a regulamentação do Marco Civil tratou dessa questão e definiu o conceito de "dado pessoal". Porém, como visto na primeira seção deste

[16] A expansão contemporânea da vigilância, onde o monitoramento torna-se uma parte cada vez mais rotineira de nossas vidas, representa uma tremenda mudança no equilíbrio do poder entre os cidadãos e as organizações. Talvez o maior perigo dessa situação seja como nossas práticas de vigilância existentes podem ser transformadas em usos opressivos. (Livre tradução)

artigo, alguns autores entendem que o direito à proteção de dados pessoais está envolta no direito à privacidade, posicionamento não unânime entre os doutrinadores.

Na segunda seção da pesquisa, foi exposto e analisado o caso *Microsoft Corporation* v. *The United States Department of Justice* e Loretta Lynch. A empresa ingressou com uma ação judicial contra o governo norte-americano para obter o direito de informar aos seus usuários do serviço de computação em nuvem, que as suas informações e dados estavam sendo acessados pelo governo, amparado pela *section* 2705 (b) do *Electronic Communications Privacy Act* de 1986. A *Microsoft* requereu a declaração de inconstitucionalidade dessa norma por violar a Primeira e a Quarta Emendas da Constituição daquele país.

Muito embora o caso ainda se encontre em fase inicial, a partir dele é possível constatar que o governo norte-americano não se intimidou com as repercussões do caso Snowden ao redor do mundo, e persiste espionando e vigiando pessoas, empresas e ações de outros Estados. Por óbvio que o Brasil não está imune à vigilância estadunidense e, por essa razão, na última seção do trabalho foram verificadas as potencialidades do Marco Civil da *Internet* em tutelar os internautas brasileiros.

O exame da legislação evidenciou que o Marco Civil comtempla o direito à privacidade e proteção de dados pessoais em seu texto, especialmente após sua regulamentação, mas não especifica medidas claras e efetivas para barrar e/ou combater a *ciberespionagem* e *cibervigilância* de outros países. Ademais, apontamentos de organizações não-governamentais estrangeiras denunciam que o Brasil investiu em respostas militares e na doutrina da guerra *cibernética*, o que pode levá-lo a cometer os mesmos erros que o governo norte-americano cometeu. Alguns autores temem pelo uso opressivo desses mecanismos.

Até pelos limites da resposta normativa percebe-se que não existe no país uma proteção suficiente aos dados pessoais contra a espionagem e vigilância governamental, especialmente aquela vorazmente implementada pelos Estados Unidos. Este quadro de incertezas aponta para a necessidade de estudo e análise constante do tema pela academia, cuja contribuição tanto pode ocorrer pela produção de pesquisas capazes de desvelar as situações de violação à privacidade, quanto pelo papel de articuladora dos demais atores (empresas, sociedade civil, organizações não-governamentais e governo brasileiro) conclamando todos à defesa da vida privada e da proteção dos dados pessoais na sociedade em rede.

REFERÊNCIAS

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza Abreu. **Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais.** Relatório elaborado pela Associação InternetLab de Pesquisa em Direito e Tecnologia em parceria com a *Electronic Frontier Foundation*, 2015. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf>. Acesso em: 14 mai. 2016.

ARTICLE 19. **Da cibersegurança à ciberguerra:** o desenvolvimento de políticas de vigilância no Brasil. Disponível em: <https://www.article19.org/data/files/medialibrary/38291/Da-Ciberseguranc%CC%A7a-a%CC%80-Ciberguerra.pdf>. Acesso em: 14 mai. 2016.

BARBOSA, Marco A.. Marco civil da internet: mercado e estado de vigilância. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo II:** Marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BONAVIDES, Paulo. **Curso de direito constitucional.** 26. ed. São Paulo: Malheiros Editores Ltda., 2011.

BRASIL. **Código Civil.** Lei n. 10.406, de 10 de Janeiro de 2002. Publicada no Diário Oficial da União, de 11-1-2002. Vade Mecum OAB e concursos. 8. ed. São Paulo: Saraiva, 2016.

_____. Comitê Gestor da Internet no Brasil. **Relatório de políticas de internet:** Brasil 2011. São Paulo, 2012. Disponível em: <http://www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf>. Acesso em: 09 mai. 2016.

_____. **Constituição da República Federativa do Brasil.** Publicada no Diário Oficial da União n. 191-A, de 5-10-1988. Vade Mecum OAB e concursos. 8. ed. São Paulo: Saraiva, 2016.

_____. **Declaração Universal dos Direitos Humanos de 1948.** UNIC/Rio, Janeiro de 2009. Disponível em: <http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>. Acesso em: 02 mai. 2016.

_____. **Decreto n. 8.771, de 11 de maio de 2016.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm#art22>. Acesso em: 14 mai. 2016.

_____. **Marco Civil da Internet.** Lei n. 12.965, de 23 de abril de 2014. Publicada no Diário Oficial da União, de 24-4-2014. Vade Mecum OAB e concursos. 8. ed. São Paulo: Saraiva, 2016.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição.** 7. ed. Coimbra: Edições Almedina, 2003.

CASTELLS, Manuel. **A galáxia internet:** reflexões sobre internet, negócios e sociedade. Tradução de Rita Espanha. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

_____. **O poder da comunicação.** Tradução de Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2013.

DANTAS, André. A sociedade da vigilância. **AUTOentusiastas.** 03 abr. 2016. Disponível em: <http://www.autoentusiastas.com.br/2016/04/sociedade-vigilancia/>. Acesso em: 08 mai. 2016.

DE LUCCA, Newton. Marco civil da internet – uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo I:** marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

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

GREENWALD, Glenn. **Sem lugar para se esconder:** Edward Snowden, a NSA e a espionagem do governo americano. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

HAGGERTY, Kevin D.. What's wrong with privacy protections? Provocations from a fifth columnist. In: SARAT, Austin (editor). **A world without privacy:** what law can and should do? New York – USA: Cambridge University Press, 2015.

LASH, Scott. **Crítica de la información.** Traducción de Horacio Pons. Buenos Aires: Amorrortu, 2005.

LEMOS, Ronaldo. Uma breve história da criação do Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo I:** marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2011.

LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do marco civil da internet a partir da *human computer interaction* e da *privacy by default*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo I:** marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

LYON, David. **Surveillance after Snowden.** Cambridge, UK: Polity Press, 2015.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 10. ed. São Paulo: Saraiva, 2015.

MEYER-PFLUG, Samantha Ribeiro; LEITE, Flavia Piva Almeida. A liberdade de expressão e o direito à privacidade no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito e internet III – Tomo I:** marco civil da internet (lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

NISSENBAUM, Helen. **Privacidad amenazada:** tecnología, política y la integridad de la vida social. Tradujo: Enrique Mercado. México: Editorial Océano, 2011.

PÉREZ-LUÑO, Antonio Henrique. Internet y los derechos humanos. **Derecho y conocimiento**, vol.2, pags. 101-121, ISSN 1578-8202. Facultad de Derecho. Universidade de Huelva, 2002. Disponível em: <http://rabida.uhu.es/dspace/bitstream/handle/10272/2550/b15616630.pdf?sequence=1>. Acesso em: 21 mai. 2016.

_____. **Los derechos humanos en la sociedad tecnológica.** Madrid: Editorial Universitas, 2012.

PILATI, José Isaac; OLIVO, Mikhail Vieira Cancelier de. Um novo olhar sobre o direito à privacidade: caso Snowden e pós-modernidade jurídica. **Seqüência:** Estudos Jurídicos e Políticos. Florianópolis, v. 35, n. 69, p. 281-300, dez. 2014. ISSN 2177-7055. Disponível em: < https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2014v35n69p281/28392>. Acesso em: 06 mai. 2016.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Direitos da personalidade.** São Paulo: Atlas, 2011.

UNITED STATES OF AMERICA. United States District Court, Western District of Washington, At Seattle. **Microsoft Corporation v. The United States Department of Justice, and Loretta Lynch, in her oficial capacity as Attorney General of the United States.** Dated this 14th day of April, 2016. Disponível em: <https://mscorpmedia.azureedge.net/mscorpmedia/2016/04/ECPA-Complaint.pdf>. Acesso em: 06 mai. 2016.

_____. United States Senate. **Constitution of the United States.** Disponível em: <http://www.senate.gov/civics/constitution_item/constitution.htm#amendments>. Acesso em: 06 mai. 2016.

VELTE, Anthony T.; VELTE, Toby J.; ELSENPETER, Robert. **Cloud computing:** computação em nuvem – uma abordagem prática. Rio de Janeiro: Alta Books Editora, 2012.

WOLTON, Dominique. **La outra mundialización:** los desafíos de la cohabitación cultural global. Traducción Irene Agoff. Barcelona: Gedisa Editorial, 2004.