UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE DIREITO

VIGILÂNCIA NA SOCIEDADE EM REDE: A COLETA DE DADOS PESSOAIS NA INTERNET E SUAS IMPLICAÇÕES AO DIREITO À PRIVACIDADE

MONOGRAFIA DE GRADUAÇÃO

Eduardo Steffenello Ghisleni

SANTA MARIA, RS, BRASIL

2015

VIGILÂNCIA NA SOCIEDADE EM REDE: A COLETA DE DADOS PESSOAIS NA INTERNET E SUAS IMPLICAÇÕES AO DIREITO À PRIVACIDADE

Eduardo Steffenello Ghisleni

Trabalho de Conclusão de Curso apresentado à Disciplina de Monografia II, do Curso de Direito da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Bacharel em Direito**.

Orientador: Prof. Dr. Rafael Santos de Oliveira

SANTA MARIA, RS, BRASIL

2015

Universidade Federal de Santa Maria
Centro de Ciências Sociais e Humanas
Curso de Direito

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Conclusão do Curso de Graduação

VIGILÂNCIA NA SOCIEDADE EM REDE: A COLETA DE DADOS PESSOAIS NA INTERNET E SUAS IMPLICAÇÕES AO DIREITO À PRIVACIDADE

elaborado por
Eduardo Steffenello Ghisleni

como requisito parcial para obtenção do grau de
Bacharel em Direito

COMISSÃO EXAMINADORA:

Rafael Santos de Oliveira
(Presidente/Orientador)

Valéria Ribas do Nascimento
(Professora UFSM)

Bruno Barros
(Mestrando UFSM)

Santa Maria, 02 de dezembro de 2015.

RESUMO
Trabalho de Conclusão de Curso de Graduação
Centro de Ciências Sociais e Humanas
Universidade Federal de Santa Maria

VIGILÂNCIA NA SOCIEDADE EM REDE: A COLETA DE DADOS PESSOAIS NA INTERNET E SUAS IMPLICAÇÕES AO DIREITO À PRIVACIDADE

Autor: Eduardo Steffenello Ghisleni
Orientador: Rafael Santos de Oliveira
Data e Local da Defesa: Santa Maria, 02 de Dezembro, de 2015.

O surgimento da internet determinou uma transformação nos mecanismos de coleta e difusão de informações. Com a expansão das formas de vigilância, as leis que protegem a privacidade tornaram-se insuficientes. Diante disso, o presente trabalho objetivou analisar a atual onda de vigilância possibilitada pela coleta de dados através da internet, especialmente no que tange à violação da privacidade de dados pessoais. Eis que, surge o seguinte problema: a atual dimensão assumida pela vigilância indiscriminada faz a sociedade caminhar para o fim do direito à privacidade? Para resolver esta questão, abordou-se, em um primeiro momento, o contexto de intensificação da vigilância e seus efeitos sobre os direitos à privacidade e à proteção de dados. Em seguida, com base nas revelações de Edward Snowden, examinou-se a vigilância governamental, verificando a necessidade de repensar o equilíbrio entre o direito à privacidade e a defesa da segurança pública. Para tanto, o estudo realizou-se através do método de abordagem dialético, apurando o caráter conflitante do tema, na medida em que, tem-se um alegado interesse público na coleta de dados (segurança pública) e, ao mesmo tempo, a necessidade da preservação da privacidade. Os métodos de procedimentos, por sua vez, foram o histórico, o monográfico e o comparativo. O primeiro, na investigação do contexto que possibilitou os atuais sistemas de vigilância. O segundo, na análise das tecnologias de vigilância, problemas gerados e possíveis soluções. Já o terceiro procedimento foi utilizado para estabelecer o contraponto entre proteção da segurança pública e preservação da privacidade com base nas justificativas apresentadas. Ao final, constatou-se, que embora o ambiente tecnológico seja hostil à privacidade, o surgimento de uma nova consciência global tem proporcionado novos caminhos para manutenção deste importante direito.

Palavras-chave: Vigilância na internet. Coleta de dados pessoais. Privacidade.

ABSTRACT
Graduation Monografh
Law School
Federal University of Santa Maria

SURVEILLANCE IN SOCIETY NETWORKING: THE COLLECTION OF PERSONAL DATA ON THE INTERNET AND ITS IMPLICATIONS TO THE RIGHT TO PRIVACY

Author: Eduardo Steffenello Ghisleni
Adviser: Rafael Santos de Oliveira
Date and Place of the Defense: Santa Maria, December 2, 2015.

The emergence of the Internet led to a transformation in the mechanisms for the collection and dissemination of information. With the expansion of surveillance forms, the laws protecting privacy have become insufficient. Therefore, this study aimed to analyze the current wave of surveillance made possible by collecting data over the internet, especially with regard to the breach of personal data privacy. Behold, the next problem arises: the current dimension assumed by indiscriminate surveillance in society is moving towards the end of the right to privacy? To address this issue, if approached, at first, the context of enhanced surveillance and its effect on the rights to privacy and data protection. Then, based on the revelations of Edward Snowden, looked to government surveillance, checking the need to rethink the balance between the right to privacy and the protection of public safety. To this end, the study was conducted through the dialectical method of approach, investigating the conflicting nature of the subject, in that, there is an alleged public interest in data collection (public security) and at the same time, the need the preservation of privacy. The methods of procedures, in turn, were the historical, the monographical and the comparator. The first, in investigating the context in which the current surveillance systems emerged. The second, in the analysis of surveillance technologies, generated problems and possible solutions. The third procedure was used to establish the contrast between public safety protection and preservation of privacy based on the justifications presented. Finally, it was found that although the technology environment is hostile to privacy, the emergence of a new global consciousness has provided new ways to maintain this important right.

Keywords: Surveillance on the Internet. Personal data collection. Privacy.

SUMÁRIO

INTRODUÇÃO

A internet revolucionou o mundo transformando as formas de interação e estabelecendo uma nova realidade social. No entanto, a mesma evolução da tecnologia de comunicação que transformou a vida das pessoas e das empresas, possibilitando o acesso mais rápido às informações e a sua socialização, culminou em sérios perigos à privacidade, eis que, expõe os indivíduos a uma visibilidade permanente.

A vigilância tornou-se um aspecto cada vez mais presente nas vidas das pessoas e tem se expandido silenciosamente nas últimas décadas através de legislações permissivas com relação à coleta de dados por meio da internet. Esta prática vem sendo estimulada tanto por governos sob a justificativa da segurança pública, quanto pelo marketing inovador das empresas de tecnologia.

Hoje, uma característica básica das sociedades modernas, e fácil de perceber, é que poucas pessoas têm realmente consciência do real alcance da vigilância a que estão submetidas e de como podem ser afetadas por ela. A ignorância da população a respeito do assunto tem contribuído para o abuso de poder dos governos e das empresas privadas, detentores das tecnologias capazes de violar uma série de direitos individuais, em especial, o direito à privacidade.

Os problemas ocasionados pela vigilância na sociedade atual englobam uma gama de novos conceitos e tecnologias como: o monitoramento de imagem através de câmeras em locais públicos, monitoramento de telefones móveis, identificação biométrica ou através de DNA, *Big Data*, sistemas de geolocalização, interceptação de dados. Essas tecnologias e conceitos representam as mais variadas formas de vigilância, porém, neste trabalho optou-se por concentrar análise nos aspectos relacionados à vigilância em massa, que envolve a coleta e tratamento indiscriminados de dados pessoais através da rede mundial e tem sido praticada tanto por empresas privadas quanto por órgãos públicos.

A crescente expansão da indústria da vigilância colocou as pessoas em uma situação de vulnerabilidade diante do constante monitoramento pelas florestas digitais. Portanto, entender o que está ocorrendo no mundo da vigilância tornou-se um desafio para qualquer pessoa e em especial para a área jurídica. Dessa forma, é

necessário que os pensadores e operadores do direito estudem arduamente as novas tecnologias e suas implicações a fim de possibilitar que o avanço tecnológico evolua em harmonia com os princípios que regem a boa convivência social.

Nesse contexto, o presente trabalho objetivou ampliar a compreensão acerca da atual onda de vigilância mundial, analisando as causas e as consequências sociais e jurídicas da coleta indiscriminada de dados pessoais, verificando se a vigilância massiva conduzirá a sociedade para o fim do direito à privacidade.

Para tanto, no primeiro capítulo do presente trabalho, optou-se por contextualizar a vigilância na sociedade atual, assim como as modificações legislativas pós 11 de setembro de 2001 que permitiram o surgimento da atual coleta massiva de dados através da internet, traçando ainda, um panorama acerca da importância do direito à privacidade e da atual regulamentação brasileira aplicável à proteção de dados pessoais. Já no segundo capítulo, promoveu-se uma análise acerca da vigilância governamental (praticada por governos), com base nas denúncias de Edward Snowden, em seguida, procurou-se verificar a necessidade de repensar o equilíbrio entre o direito à privacidade e a defesa da segurança pública, para então debater as propostas mais relevantes visando anular ou minimizar os danos ocasionados por este tipo de vigilância e preservar o direito à privacidade.

A realização do presente estudo fez uso do método de abordagem dialético, verificando o caráter conflitante do tema submetido à pesquisa, na medida em que, tem-se um alegado interesse público na coleta de dados (segurança pública), e ao mesmo tempo, tem-se a necessidade da preservação do direito à privacidade.

Por sua vez, os métodos de procedimento utilizados foram o histórico, o monográfico e o comparativo. O primeiro, na investigação do contexto jurídico e social que possibilitou o surgimento de poderosos sistemas de vigilância. O segundo procedimento visando analisar as tecnologias de vigilância, os problemas gerados e as propostas de soluções. Já o terceiro procedimento foi utilizado para estabelecer o contraponto entre a necessidade de proteção da segurança pública e a preservação do direito à privacidade com base nas justificativas conflitantes em cada caso.

Desse modo, verifica-se a relevância de tal estudo não apenas por se tratar de uma questão de amplo interesse público e político, mas principalmente, pela urgente necessidade de proteção de um direito tão fundamental quanto a privacidade frente à implacável evolução tecnológica.

1 A ERA DA VIGILÂNCIA E O CONTEXTO DE EROSÃO DA PRIVACIDADE DE DADOS PESSOAIS

O avanço tecnológico – após surgimento da internet – aliado a uma série de acontecimentos mundiais que despertaram uma busca intensa por segurança, originou uma onda de vigilância por todo mundo e uma corrida pela coleta do fluxo de informações.

A coleta de informações, seja com interesses públicos ou privados, se tornou algo tão comum e difundido que deu origem a expressões como “Era da Vigilância” ou “Vigilância Digital” para descrever o atual momento, em que tanto empresas, quanto estados soberanos, dispondo de altas tecnologias, passaram a fazer uso de poderosos sistemas de vigilância.

Em tempos em que se busca a consideração do acesso à internet como um direito fundamental (GOULART, 2012), a rápida evolução tecnológica que possibilitou a coleta massiva e sistemática de informações através das redes de comunicação, acaba por promover a violação de uma série de direitos individuais. A tal ponto, que os próprios conceitos de público e privado foram alterados de forma radical e passaram a ser definidos por limites cada vez mais frágeis.

Conforme Zygmunt Bauman, no livro intitulado Vigilância Líquida, a informação passou a ser um bem valioso para definição de estratégias de *marketing* e publicidade das organizações privadas. Segundo o autor, na era digital, em que o status do consumidor se altera a cada novo bit de informação transacional, suas chances de tornar-se alvo de alguma forma variam de acordo com os níveis de tráfego e a trilha de rastros mais recente que deixou pra trás (BAUMAN, 2013).

Antes de abordar o fenómeno complexo da vigilância, na sociedade atual, torna-se importante considerar algumas definições de seu conceito. Michel Foucault, ao analisar a visão do Panóptico, concebida pelo filósofo inglês Jeremy Bentham, associa a vigilância a formas de controle em espaços fechados onde pessoas estão confinadas, como prisões, asilos, hospitais, ou locais de trabalho (FOUCAULT, 1987). Segundo Anthony Giddens, a vigilância pode ser definida como “a codificação de informações relevantes para a administração de uma população de sujeitos, mais a direta supervisão destes por funcionários e administradores de todos os tipos”

(GIDDENS, 1984, p. 183-184). Já uma definição mais detalhada é a apresentada por Christian Fuchs:

> Minha visão pessoal é de que a informação é um conceito mais geral do que a vigilância e que a vigilância é um tipo específico de recuperação de informação, armazenamento e processamento, avaliação e uso que envolve dano potencial ou real, coerção, violência, relações de poder assimétricas, controle, manipulação, dominação, poder disciplinar. É um instrumental e um meio de tentar extrair e acumular benefícios para certos grupos de indivíduos às custas de outros grupos ou indivíduos. A vigilância está baseada numa lógica de competição. Ela tenta fazer florescer ou evitar certos comportamentos de grupos ou indivíduos reunindo, armazenando, processando, difundindo, avaliando e usando informação sobre seres humanos de forma que a violência física, ideológica ou estrutural, potencial ou real, pode ser direcionada aos humanos de forma a influenciar seu comportamento. (FUCHS, 2011, p. 129)

Nota-se, que estabelecer uma definição única para a vigilância é uma tarefa muito difícil, pois cada conceito se baseia em questões teóricas abstratas e bastante específicas. No entanto, neste momento não é importante estabelecer uma definição para a vigilância, mas sim, possibilitar o entendimento do significado da vigilância em massa, no qual se concentra o presente estudo.

Para tanto, com base na descrição apresentada pela *Privacy International* – organização comprometida com a luta pelo direito à privacidade ao redor do mundo – considera-se a vigilância em massa como a sujeição de uma população ou componente importante de um grupo ao monitoramento indiscriminado. Tratando-se de uma interferência sistemática ao direito das pessoas à privacidade. Geralmente é feita por governos, podendo também ser feita por empresas a pedido de governos ou por iniciativa própria. Assim, qualquer sistema que gera e coleta informações sobre os indivíduos sem tentar limitar o conjunto de dados para indivíduos alvo bem definidos é uma forma de vigilância em massa (PRIVACY INTERNATIONAL, 2015).

Percebe-se, portanto, que a vigilância em massa é talvez o principal elemento caracterizador da atual “Era da Vigilância”, em que a vigilância passou a ser praticada indiscriminadamente sobre todo tipo de pessoa ou informação, o tempo todo. Dessa forma, o fluxo de informações pessoais foge do controle de seu titular, colocando-o em uma situação de vulnerabilidade frente às empresas ou ao próprio governo, principais praticantes da coleta massiva de dados pessoais.

Assim, a atual superexposição de informações pessoais, aliada ao fato de que a internet não "esquece" nada, levanta uma série de questionamentos acerca do

possível fim da privacidade e do direito que lhe corresponde. A internet abriu o mundo para as pessoas, mas ela também abriu as pessoas para o mundo. E cada vez mais, o preço a se pagar por toda esta conectividade é a perda ou redução de direitos, especialmente o direito à privacidade.

Convém ressaltar, que o avanço tecnológico proporcionou a todos grandes vantagens, além de uma série de comodidades através da possibilidade de comunicações em tempo real. Portanto, o que se pretende ao analisar a vigilância moderna não é negar os benefícios evidentes, mas sim, estabelecer qual o preço dessas vantagens para os indivíduos e os possíveis mecanismos jurídicos capazes de proteger direitos tão importantes para a sociedade.

> As inúmeras e generosas lei que protegem a privacidade ficam esvaziadas perante a agressividade das práticas comerciais ou não, provenientes da circulação dos dados informáticos. Em decorrência desses fatos, surge a necessidade da proteção legislativa específica do direito ao controle sobre as próprias informações. (PAESANI, 2012, p.37)

Neste sentido, é importante ressaltar o papel da proteção de dados pessoais como mecanismo jurídico essencial para a concretização do direito à privacidade, especialmente no ordenamento jurídico brasileiro.

> No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada. (DONEDA, 2011, p. 103)

Neste capítulo, analisar-se-á o contexto jurídico e social que possibilitou a o surgimento dos poderosos sistemas de vigilância da atualidade, assim como, uma reflexão acerca das modificações conceituais sofridas pela privacidade a partir da implementação da coleta massiva de dados pessoais em grandes empresas de tecnologia. Por fim, será feita uma análise da legislação brasileira sobre a proteção de dados.

1.1 Ampliação da coleta de dados na internet

Com o advento da Internet, o cotidiano das pessoas foi alterado por tecnologias que permitiram o acesso e socialização de informações de forma rápida, imprimindo maior dinamicidade às relações econômicas, à participação política e às interações sociais. Não obstante os inúmeros benefícios do avanço tecnológico, a evolução dos mecanismos de coleta e o tratamento de informações pessoais alcançaram um patamar potencialmente nocivo à privacidade.

Na atualidade, empresas e governos empregam modernas tecnologias para rastrear e sistematicamente coletar informações através da internet (MARQUES; PINHEIRO, 2014, p. 47). No entanto, considerando-se o período de mais de 30 anos desde o surgimento da Internet, percebe-se que nem sempre ela esteve altamente permeada por ferramentas de vigilância.

Foi após os acontecimentos de 11 de setembro de 2001, que a intensificação da vigilância, em todos os aspectos sociais, tornou-se uma tendência mundial. Enquanto as nações mundo a fora reforçavam a ideia do uso de sistemas de vigilância para manter a segurança nacional e afastar o temor de um novo ataque terrorista, uma nova onda de controle dominava quase todas as cidades sem nem ao menos ser notada (LYON, 2007, p. 11-12).

Após os ataques terroristas ao *World Trade Center*, o governo dos Estados Unidos passou a alterar as legislações sobre proteção de dados e investir fortemente em sistemas de vigilância. Tudo isso, em meio a uma aceitação passiva de cidadãos amedrontados e tomados por uma sensação de insegurança. Segundo Silva (2006, p. 4), “o 11 de Setembro apenas foi o perfeito pretexto para legitimar as tensões sempre existentes entre a defesa da privacidade e a propensão para a implementação de severas medidas de segurança”.

Assim, o anúncio de uma “Guerra ao Terror” deu início a uma série de medidas legislativas no governo dos Estados Unidos que influenciaram e modificaram a regulamentação da coleta e tratamento de dados na internet. Esse conjunto de medidas legislativas foi chamado de Ato Patriota (*Patriot Act, em inglês*).

O Ato Patriota, assinado pelo então presidente George W. Bush, em 26 de outubro de 2001, permitiu uma série de medidas extremas como interceptação de ligações telefônicas e e-mails pelos órgãos de inteligência e segurança sem a

necessidade de autorização da Justiça, assim como, o “direito” de obter informações das empresas americanas acerca dos registros dos usuários (ESTADOS UNIDOS, 2001).

Dessa forma, sob a justificativa de fornecer as ferramentas necessárias para interceptar e obstruir atos terroristas, o governo dos Estados Unidos impôs às empresas de telefonia e internet que passassem a armazenar todo tipo de dados dos usuários.

As modificações legislativas, somadas a um enorme senso de oportunidade para um *marketing* inovador, serviram para impulsionar as empresas a tornarem-se especialistas na coleta de dados. A ponto de, atualmente, criarem “perfis” de seus usuários extremamente detalhados, contendo desejos, interesses, preferências, opiniões e diversas outras informações pessoais.

Para o entendimento das transformações ocorridas na coleta e tratamento de dados no ambiente virtual é importante considerar o caráter de autorregulamentação que sempre predominou na internet, através dos termos ou políticas de uso específicas de cada endereço eletrônico.

> De uma forma geral, a maneira como os dados do usuário são tratados pelos sistemas está prevista nas normas que regulam o seu uso. Estas normas, geralmente descritas em documentos denominados ‘Termo de Uso’ ou ‘Política de Uso’, demandam adesão para possibilitar o acesso aos serviços. (MIRANDA; SOUSA, 2015, p. 30)

Essas disposições legais servem para balizar a ação dos serviços de internet; a maneira como são utilizados os sistemas de informação; e também para deixar claro aos usuários quais seriam os limites, tornando transparentes e seguras as adesões aos serviços e as relações daí decorrentes.

Portanto, o contexto social e jurídico provocou uma mudança de comportamento das empresas, que precisaram alterar suas políticas de privacidade, pois elas, até então, limitavam o uso de dados pessoais, preservavam a privacidade de seus usuários, sendo que, visavam mantê-los como clientes.

Para verificar as alterações sistemáticas sofridas por políticas de privacidade, e tomando o Google como exemplo, optou-se por comparar trechos específicos em seus regulamentos em diferentes anos. A análise dos textos denota como estes regulamentos ficaram mais complexos e permissivos em relação à coleta e manipulação de dados pessoais dos usuários com o passar dos anos.

> **Política de Privacidade do Google no ano 2000:**
> O Google respeita e protege a privacidade dos indivíduos que utilizam os serviços do motor de busca do Google. Individualmente informações identificáveis sobre você não são deliberadamente divulgadas a qualquer terceiro sem a sua permissão prévia [...]
> O Google **não coleta qualquer informação pessoal** sobre você (como seu nome, endereço de e-mail, etc.) **exceto quando você especificamente e conscientemente fornecer tais informações**. (WAYBACKMACHINE, [2000?], tradução nossa, **grifo nosso**)

> **Política de Privacidade do Google no ano 2005:**
> Quando você assina uma Conta do Google ou outro serviço do Google ou promoção que requer cadastramento, nós solicitamos informação pessoal (tal como nome, endereço de e-mail e uma senha de conta) [...] **Podemos combinar a informação que você submete em sua conta com a informação de outros serviços** do Google ou terceiros a fim de fornecer-lhe uma experiência de navegação melhor e para melhorar a qualidade de nossos serviços. (GOOGLE, 2005, **grifo nosso**)

> **Política de Privacidade do Google em 2015:**
> Quando o usuário abre uma conta, pedimos informações pessoais, como nome, endereço de e-mail, número de telefone ou cartão de crédito para armazenar com a conta. [...]
> **Coletamos informações sobre os serviços que o usuário utiliza e como os usa,** por exemplo, quando assiste a um vídeo no YouTube, visita um website que usa nossos serviços de publicidade ou quando vê e interage com nossos anúncios e nosso conteúdo. [...]
> **Coletamos informações específicas de dispositivos** (por exemplo, modelo de hardware, versão do sistema operacional, identificadores exclusivos de produtos e informações de rede móvel, inclusive número de telefone). A Google **pode associar identificadores** de dispositivo ou número de telefone à Conta do Google do usuário. [...]
> Quando o usuário utiliza os serviços da Google, **podemos coletar e processar informações sobre a localização real dele**. [...] (GOOGLE, 2015, **grifo nosso**)

Nota-se, portanto, que a política de privacidade do Google no ano 2000 (antes dos atentados terroristas) – prevendo que não seriam coletados dados pessoais, exceto quando deliberadamente fornecidos, nem divulgados a terceiros sem permissão prévia – em muito difere da política de privacidade atual, em que o Google coleta todo tipo de informações e muito pouco ou nada estabelece no sentido de proteger a privacidade dos usuários.

Outro ponto a ser destacado é o fato de que as pessoas não costumam ler os termos de uso e políticas de privacidade dos serviços que utilizam. Isso faz com que elas acabem abrindo mão da privacidade, ao aderir a termos que permitem a utilização dos dados coletados das mais variadas formas. E isso acontece principalmente porque a quantidade de informação a ser analisada é gigantesca

considerando a enorme quantidade de serviços e aplicativos que as pessoas costumam utilizar.

Para exemplificar o grande volume de termos a serem analisados em um caso concreto, com a ajuda de um editor de texto realizou-se uma contagem de palavras a serem lidas e aceitas para criação de uma conta no *Facebook*. O resultado demonstra que para criar uma conta simples, uma pessoa deve concordar com Termos de Serviço (3.425 palavras), Política de Dados (2.786 palavras) e com o Uso de Cookies (2.934 palavras), o que representa uma leitura de aproximadamente 20 páginas em termos de grande complexidade para a maioria da população. Isso tudo, para apenas um serviço (FACEBOOK, 2015a, 2015b, 2015c).

Convém, no entanto, ressaltar que esse contexto de alterações em políticas de privacidades e de pressões governamentais para uma maior coleta de dados não foi o único fator que contribuiu para o surgimento dos atuais sistemas de vigilância. Antes mesmo dos atentados terroristas e da busca compulsiva por segurança, a valorização da informação já transformava a sociedade pós-moderna.

> [...] na transição da sociedade industrial para a pós-industrial, a informação vai se delineando como ingrediente indispensável à tomada de decisões e objeto propulsor do desenvolvimento, e que o fator determinante do progresso se desloca cada vez mais da posse de bens materiais para a capacidade de elaborar ideias (CABRAL, 1992, p. 214).

Uma informação pode ser valiosa por diferentes motivos e para pessoas diferentes. Para uma empresa, por exemplo, a informação é um bem de alto valor, pois proporciona a tomada de decisões precisas para obter o sucesso em seus negócios.

O mercado competitivo e o desenvolvimento tecnológico induziram as empresas a uma busca incessante pela informação. Quando a publicidade e as estratégias de *marketing* podem significar a sobrevivência no mercado, informações acerca de desejos e preferências de um público alvo representam uma enorme vantagem.

O potencial lucrativo do armazenamento de dados fez com que as empresas passassem a perceber os usuários como produtos e não mais como simples clientes. Essa mudança de percepção fez as empresas estimularem o fornecimento de informações pessoais em troca de serviços gratuitos. Siva Vaidhyanathan, estudioso de mídia e direito, comenta esse comportamento:

> Abrir mão de qualquer serviço do Google põe o usuário da rede em desvantagem ante os outros usuários. Quanto mais o Google integra seus serviços, e quanto mais interessantes e essenciais se tornam os serviços por ele oferecidos, mais importante se torna o uso do Google para o comércio, a autopromoção e a cidadania cultural. Portanto, quanto mais amplo se tornar o alcance do Google, maiores serão as probabilidades de que até mesmo os usuários mais críticos e bem informados da Internet permaneçam no universo do Google e permitam que o Google use suas informações pessoais. Para o Google, quantidade é sinônimo de qualidade. Para nós, a submissão às opções predefinidas do Google aumenta a conveniência, a utilidade e o *status*. (VAIDHYANATHAN, 2011, p.105)

Dessa forma, as pessoas vão abrindo mão da privacidade em troca de aplicativos, serviços e novas tecnologias oferecidas pelas empresas, que por sua vez vão adquirindo cada vez mais informações sobre as pessoas, obtendo vantagens competitivas, mas também, uma quantidade colossal de dados de fazer inveja a qualquer serviço de inteligência.

Com relação à coleta massiva de dados e o alcance da vigilância atual é importante destacar que as tecnologias de processamento e armazenamento de dados foram desenvolvidas a ponto de possibilitarem inclusive a obtenção de informações totalmente novas a partir dos dados coletados. Estas novas capacidades tecnológicas fizeram surgir novos conceitos como “Metadados” e “*Big Data*”, relacionados ao fenômeno dos grandes volumes de dados.

Enquanto Metadados podem ser basicamente definidos como "dados que descrevem os dados", ou seja, são informações úteis para identificar, localizar, compreender e gerenciar os dados, *Big Data* é o termo popular, em inglês, para descrever a tecnologia capaz de localizar, analisar e processar volumes gigantescos de dados em poucos segundos.

Segundo Cezar Taurion, especialista em novas tecnologias na IBM, *Big Data* ainda é um termo mal compreendido por algumas empresas, mas cada vez mais chama atenção pela impressionante velocidade em que grandes volumes de dados são criados pela sociedade (TAURION, 2013).

As novas capacidades tecnológicas certamente possuem um potencial extraordinário para aplicações positivas, como melhorias de tráfego público, prevenção de crimes e combinação de ofertas de serviços. Contudo, no mundo da coleta dados, onde a cada clique, *login* e *download*, entregam-se gigabytes de informações, tanto de forma consciente, quanto inconsciente, existem diversas consequências sociais negativas advindas da má utilização desses dados.

Portanto, é fundamental que o direito seja capaz de conferir uma proteção abrangente a todos os aspectos derivados da coleta e tratamento de dados pessoais.

1.2 A privacidade e a proteção de dados pessoais

Historicamente, o surgimento do conceito de privacidade coincide com a desagregação da sociedade feudal e com o crescimento da classe burguesa em um contexto de mudanças sociais e econômicas relacionadas à Revolução Industrial. Época em que o isolamento era privilégio de poucos. (NAVARRO, 2014)

Neste sentido, Rodotà afirma que a privacidade se configurou como uma possibilidade para a classe burguesa, e que seus instrumentos jurídicos de tutela tiveram por base a proteção da propriedade.

> Um multifacetado conjunto de condições fez com que "[...] a privacidade evoluísse como um direito típico da classe burguesa em determinados ambientes sociais. [...] A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferencia a burguesia das demais classes: e o forte componente individualista faz com que esta operação se traduza, posteriormente, em um instrumento de isolamento do indivíduo burguês em relação à sua própria classe. O burguês, em outros termos, apropria-se de um seu "espaço", com uma técnica que lembra aquela estruturada para a identificação de um direito à propriedade "solitária". Em um nível social e institucional, portanto, o nascimento da privacidade não se apresenta como a realização de uma experiência "natural" de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo. Não é por acaso que seus instrumentos jurídicos de tutela foram predominantemente modelados com base naquele característico do direito burguês por excelência: a propriedade." (RODOTÀ, 2008, p. 26-28)

Já a doutrina do direito à privacidade, conforme lembra Doneda, teve início com o famoso artigo de Samuel Warren e Louis Brandeis, intitulado *The Right to Privacy* (1890). Sendo marcada em seus primórdios por relacionar-se ao "direito de ser deixado só". Somente posteriormente esta concepção foi evoluindo para entender a privacidade como um aspecto fundamental da realização da pessoa e do desenvolvimento de sua personalidade. (DONEDA, 2006, p. 4-5)

Com a evolução tecnológica e o aumento do fluxo de informações, crescia também a importância da informação. Assim, não eram mais somente as pessoas de

grande relevo social que estavam sujeitas a terem sua privacidade ofendida, mas sim uma parcela muito maior da população, em uma gama igualmente variada de situações. Dessa maneira, conceituar a privacidade simplesmente como o direito à proteção contra as interferências alheias tornou-se um problema para algo tão vago e em constante evolução.

Segundo Doneda (2006, p. 37), por mais difícil que seja cristalizar a problemática da privacidade em um único conceito, é razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade. Podendo-se inclusive aventar a hipótese de que o advento de estruturas jurídicas e sociais que tratem do problema da privacidade são respostas diretas a uma nova condição da informação, determinada pela tecnologia.

A própria percepção da privacidade e de sua importância foi sendo alterada com o desenvolvimento social e tecnológico, de maneira que, ações que antigamente eram consideradas como altamente ofensivas a esse direito, hoje, são vistas como algo natural. Assim, o que era entendido como privacidade no final do século XIX, já não é suficiente para definir esse direito na sociedade atual (CARLONI, 2013, p. 22).

Um conceito de privacidade, mais contemporâneo, é o relacionado ao controle das informações pessoais, também chamada de “autodeterminação informativa”, que se refere ao direito que o indivíduo tem de controlar a circulação de informações que dizem respeito à sua vida (MACHADO, 2014). Este perspectiva serviu de base para o desenvolvimento das leis de proteção de dados pessoais, conforme salienta Danilo Doneda.

> O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos e é caso emblemático de uma tendência que, a princípio, parecia apenas destinada a mudar determinado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados. Esse desenvolvimento foi intenso nas cerca de quatro décadas que a disciplina ostenta. (DONEDA, 2011, p. 96)

No entanto, a capacidade de controle sobre o tratamento e captação de dados pessoais em determinadas ocasiões beira à impossibilidade em função do alcance das atuais tecnologias, pois o indivíduo perde o controle sobre as

informações, que poderão ser “descobertas” por processos complexos de análise de dados em larga escala (dados secundários) (CARLONI, 2013, p. 29).

Pode-se, portanto, considerar que o problema reside menos na definição da privacidade em si do que em determinar o que se espera desta definição. Desse modo, é importante indagar qual o estágio atual da privacidade na sociedade digital? Sobre esse ponto, é interessante citar o discurso de Mark Zukerberg, fundador do *Facebook*, em evento realizado pela *TechCrunch* (empresa especializada em mídia e tecnologia) em 2010, que ao ser questionado sobre o futuro da privacidade, afirmou que a privacidade não é mais considerada uma “norma social”, pois evoluiu com o tempo. Zukerberg argumentou ainda, que as pessoas se sentem mais confortáveis não apenas para compartilhar mais informações e de diferentes tipos, mas também de forma mais aberta e com mais pessoas (HUFFINGTON POST, 2010). A postura de Zukerberg, ao minimizar a importância da privacidade – logo após o *Facebook* ter não só reduzido o controle dos usuários sobre seus dados pessoais, como também tornado públicas muitas informações que antes eram privadas – denota não apenas o estágio de irrelevância da privacidade na atual sociedade, como também o movimento de grandes empresas no sentido de tentar diminuir sua importância.

> Na verdade, é exatamente assim que a vigilância atual deseja que as coisas transcorram. ChoicePoint, Facebook, Google e Amazon querem nos ver descontraídos, que sejamos nós mesmos. A essas empresas interessa explorar nichos de mercado criados por nossas opções de consumo. Elas se empenham em rastrear nossas singularidades porque entendem que o modo como tentamos nos diferenciar da grande massa reflete exatamente as coisas que mais apreciamos. Nossas paixões, predileções, fantasias e fetiches constituem aquilo em que somos mais propensos a gastar nossas economias e que, por esse motivo, nos transformam em alvos fáceis das boas estratégias de marketing. (VAIDHYANATHAN, 2011, p.128)

O mundo passa por uma revolução digital e tecnológica. *Big Data*, câmeras de vigilância por toda parte, *drones* cada vez menores, reconhecimento facial (identificação biométrica), rastreamento e localização de celulares, são apenas alguns exemplos de tecnologias que fazem a privacidade sofrer uma prolongada e implacável agonia. Nesse contexto, surgem duas questões relevantes a serem analisadas: Qual a importância da privacidade para a sociedade? E o que fazer para preservá-la?

Verner Dittmer, ex-diretor da Siemens, em artigo publicado em 2006 pelo jornalista Ethevaldo Siqueira, no jornal Estado de São Paulo, argumenta que em um mundo sem privacidade haverá menos impunidade, um dos grandes problemas do Brasil. Segundo ele, além disso, a justiça e os negócios serão mais rápidos, pois baseados em fatos e não em opiniões, logo, não se deve lamentar a morte desse suposto direito, pois isso até poderá ser bom para a sociedade (SIQUEIRA, 2006).

Por outro lado, basta uma reflexão um pouco mais profunda para perceber que a privacidade tem uma função de apoio para o exercício de outras garantias e direitos fundamentais, como a liberdade de expressão e reunião, que conjuntamente apoiam o funcionamento da democracia.

Em conferência promovida pelo TED (*Technology, Entertainment and Design*) em 2014, na palestra intitulada "*Por que a privacidade é importante*", Glenn Greenwald, argumenta que quando as pessoas estão sendo monitoradas ou observadas mudam radicalmente seus comportamentos, assim, as possibilidades de comportamentos variados se reduzem drasticamente pelo fato de acharem que estão sendo observadas. Dessa forma, uma sociedade em que as pessoas podem ser monitoradas o tempo todo alimenta a passividade, obediência e submissão, razão pela qual todo tirano, do mais declarado ao mais sutil, deseja esse sistema, pois somente quem estiver disposto a se tornar suficientemente inofensivo para quem detêm o poder político é que pode estar livre dos perigos da vigilância (TEDGLOBAL, 2014).

Então, como preservar a privacidade na era da vigilância? Uma pergunta como essa não possui resposta fácil, o que reforça a necessidade de estudos e de novas abordagens acerca do tema. Segundo Marcel Leonardi (2011), estão surgindo diversas novas correntes doutrinárias abordando esta problemática, como por exemplo, a que defende a utilização de um sistema jurídico em conjunto com a arquitetura da própria internet.

> A idéia de regulação por meio da arquitetura é óbvia em alguns contextos: para evitar que carros trafeguem em alta velocidade nas proximidades de escolas, lombadas são construídas nas ruas que as circundam; obstáculos são colocados junto a escadas rolantes em aeroportos, para evitar que passageiros levem carrinhos de bagagens a certos locais; e filas são organizadas, por meio de barreiras físicas. (LEONARDI, 2011, p. 162)

A analogia faz referência aos “mecanismos tecnológicos sobrepostos às características originais da Rede que intencionalmente restringem o comportamento de seus usuários, forçam certas condutas, ou possibilitam coibir determinadas práticas.” (LEONARDI, 2011, p. 178), ou seja, atuam em conjunto com o sistema jurídico.

Um aspecto importante a ser considerado é o fato de que a privacidade tem saído da esfera puramente privada e ganhado formas coletivas que demandam novos métodos de análise e tutela. Essa tendência à mudança dos sujeitos que demandam pela privacidade, com a inclusão de classes menos privilegiadas decorrentes da inclusão digital proporcionada pela tecnologia deve ser considerada para produção de leis realmente eficazes na sociedade atual.

> Desta dimensão coletiva surge, enfim, a conotação contemporânea da proteção da privacidade, que manifesta-se sobretudo (porém não somente) através da proteção de dados pessoais. (DONEDA, 2006, p. 18)

Constata-se, pois, que a elaboração de leis para preservação das garantias individuais afetadas pelo amplo desenvolvimento das tecnologias de vigilância passa necessariamente por uma eficiente regulamentação acerca da proteção de dados no ambiente digital.

Em se tratando de dados pessoais no meio virtual, a coleta de informações pessoais pode ocorrer tanto pela disponibilização espontânea em redes sociais, blogs e cadastros para acesso a serviços na internet, quanto pela captura através de programas geralmente ocultos que rastreiam toda navegação e comportamento dos usuários. Dessa forma, a exposição pessoal pode acontecer tanto conscientemente pela divulgação direta de informações, quanto inconscientemente pela obtenção indireta de dados pessoais, o que aumenta muito os riscos de um indivíduo ter direitos violados. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p. 85-91)

Para Doneda, os efeitos das violações de privacidade ganham tais dimensões que acabam por aumentar a necessidade de se criar um eixo em torno do qual estruturar a proteção deste direito, criando uma necessidade real e não apenas acadêmica de se buscar um mínimo conteúdo comum para o direito à privacidade que harmonize o tratamento da privacidade em diversas sociedades. O autor exemplifica ainda, que atualmente uma pessoa deve se preocupar não somente com notícias indiscretas sobre festas familiares que possam ser publicadas no jornal da

cidade, mas também com as informações que uma empresa de assistência médica tem, em *Hong Kong*, sobre informações genéticas e hábitos alimentares de sua pessoa (DONEDA, 2006, p. 86).

No mesmo sentido, as pesquisadoras da Microsoft Kate Crawford e Danah Boyd, alertam que as consequências da manipulação dos dados podem ser muito graves, especialmente para as populações minoritárias, com a inclusão de políticas discriminatórias e o acesso restrito a serviços financeiros e de saúde (BOYD, 2011).

Assim, quando as pessoas utilizam os serviços de uma empresa como *Google*, *Facebook* e *Amazon*, essas empresas coletam informações, desejos, interesses e preferências, visando exercer influência em futuras ações das pessoas. O cenário mais amplo, porém, denota que os efeitos gerais da vigilância digital, não se resumem a selecionar positivamente os consumidores satisfeitos e prometer-lhes futuros benefícios e recompensas, mas incluem selecionar negativamente os que não se conformam às expectativas, por exemplo. A segmentação de público realizada pelas grandes empresas com base em dados pessoais, mesmo que na tentativa de oferecer melhores serviços, acaba produzindo uma discriminação social, conforme exemplificado por David Lyon em debate sobre vigilância com Zygmunt Bauman:

> Sabe-se razoavelmente bem que pessoas diferentes que consultam a mesma palavra no Google obtêm resultados diferentes. Isso porque o Google refina seus resultados de buscas segundo as pesquisas anteriores. Da mesma forma, os que têm muitos amigos no Facebook só vão receber atualizações daqueles sobre os quais o próprio Facebook julga que se quer ter notícias, com base na frequência das interações com essas pessoas. (BAUMAN, 2013, p.114-115).

Em uma análise mais profunda, percebe-se que a “categorização da conduta visando à simulação de comportamentos futuros” (BRUNO, 2008, p. 14), não apenas produz divisões sociais e um tratamento diferencial, mas também, cria um enorme potencial de manipulação e controle através da manipulação de escolhas.

> Um exemplo um tanto extremo, e talvez desconcertantemente ruidoso, mas bastante característico, é fornecido pelo hábito universal das agências de namoro de arranjar os potenciais objetos de desejo segundo as preferências apresentadas pelos potenciais clientes – como cor da pele ou do cabelo, peso, tamanho dos seios, interesses declarados, passatempos favoritos etc. (BAUMAN, 2013, p. 126)

Outra questão que merece destaque diz respeito às informações relativas a opiniões políticas ou manifestações de ideais religiosos ou filosóficos, muito comuns nas redes sociais atualmente. É comum deparar-se com violações de liberdades ou emprego de métodos de controle social, especialmente em organizações em que a maior parte da regulamentação é imposta e elaborada por elas próprias.

Um exemplo recente de censura na rede foi a retira do ar pelo Facebook do texto do jornalista Patrick Cockburn, que apontava responsabilidade dos EUA na origem da onda de refugiados que chega à Europa (MARTINS, 2015).

> Se as redes sociais passam a ser uma arena de debate e de manifestação pública de discursos, deve haver um limite para as restrições impostas por ela, sob pena de se afetar a liberdade de expressão dos usuários. (GOULART, 2014, p. 98)

Os efeitos negativos advindos da atual vigilância despertam a urgente necessidade de operacionalização da proteção da privacidade. Para tanto, a proteção de dados pessoais acaba ganhando relevo, pois com a convergência de tecnologias para o meio eletrônico as diferentes formas de vigilância (física, psicológica, digital) passaram a configurar formas de vigilância sobre dados pessoais.

> A proteção dos dados pessoais compreende, basicamente, pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias – especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a conceitualística, na qual o direito à privacidade era limitado por uma tutela de índole patrimonialística, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa. (DONEDA, 2006, p. 16)

Em relação ao ordenamento jurídico brasileiro, verifica-se que o mesmo não possui uma lei específica para a proteção de dados, mas uma legislação dispersa que confere alguma garantia à privacidade. A Constituição Federal de 1988 incluiu dentre as garantias e direitos fundamentais de seu artigo 5º a proteção da “intimidade” e da “vida privada” (inciso X), deixando claro que a proteção da pessoa humana abrange estes aspectos. Apresentou ainda, sob o aspecto instrumental o remédio constitucional do *habeas data*.

Já no plano infraconstitucional existem alguns regimes setoriais de tutela, como o Código de Defesa do Consumidor, que disciplina os bancos de dados de consumo. Mas dentre as legislações mais recentes, destacam-se a Lei do Cadastro Positivo, a Lei do Acesso à Informação e o recente Marco Civil da Internet.

Com a finalidade de evitar um aprofundamento desnecessário ao estudo, alongando em demasia o texto, optou-se por elaborar um quadro (Quadro 1) apresentando uma síntese dos principais aspectos abordados por estas legislações, com a finalidade de elucidar o atual panorama da proteção de dados no Brasil, para em seguida analisar os aspectos mais relevantes envolvendo o Anteprojeto da Lei de Dados Pessoais que visa regulamentar o tema no Brasil.

Lei do Cadastro Positivo (Lei nº 12.414/2011)	Disciplina a formação e consulta a bancos de dados com informações de adimplemento, para formação de histórico de crédito, garantindo acesso a todos os dados armazenados, responsabilização sobre a atualização e correção de informações.
Lei de Acesso à Informação (Lei nº 12.527/2011)	Regula o tratamento de informações pessoais em órgãos e entidades vinculadas ao poder público ou que recebam recursos públicos, mencionando a necessidade de transparência, respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, além de, estabelecer a necessidade de autorização ou consentimento expresso da pessoa a que se referem às informações para fins de divulgação ou acesso por terceiros.
Marco Civil da Internet (Lei nº 12.965/2014)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Significa grande avanço na regulamentação de coleta, armazenamento e uso de dados pessoais, prevendo a necessidade de autorização prévia para cessão de informações a terceiros, necessidade de clareza contratual, garantia de exclusão dos dados dos usuários após o término da relação entre as partes, em caso de requerimento e a necessidade de autorização judicial para acesso a registros de conexão e navegação na internet.

Quadro 1 – Resumo dos assuntos tratados nas principais leis que regulamentam a proteção de dados no ordenamento jurídico brasileiro. (BRASIL, 2011a, 2011b, 2014)

Não é difícil perceber que a legislação brasileira vigente é insuficiente à devida proteção e regulação dos dados pessoais. E apesar do pioneirismo do Marco Civil da Internet, sancionado em abril de 2014, um fator que contribui para esta insuficiência protetiva é que a lei ainda carece de regulamentação, o que prejudica os seus efeitos práticos. Ademais, não possuir uma legislação específica sobre proteção de dados pessoais torna-se um enorme obstáculo à proteção de dados em qualquer país. Para tentar corrigir esses problemas, o governo iniciou debates públicos para a elaboração da Lei de Proteção de Dados Pessoais e do decreto presidencial que regulamentará o Marco Civil da Internet em plataformas digitais no portal do Ministério da Justiça.

O Anteprojeto da Lei de Dados Pessoais, atualmente em fase de consulta pública e que deverá ser enviado ao Congresso apenas em 2016, traz em seu texto um rol de princípios mais amplo que o Marco Civil, e visa dar ao cidadão o controle sobre seus dados pessoais, sendo que, o seu titular deverá consentir para o fluxo da informação, não importando se este dado é público ou privado, conforme o estabelecido no artigo 7° do anteprojeto (BRASIL, 2015).

> **Art. 7º** O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.
>
> [...]
>
> **§3º** O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.
>
> **§4º** O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.
>
> **§5º** O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.
>
> **§6º** O consentimento pode ser revogado a qualquer momento, sem ônus para o titular. [...]

Como se percebe, o consentimento do titular da informação deverá ser fundamental para os possíveis usos do conteúdo pessoal. Dessa forma, a proteção legal para que as informações somente possam ser armazenadas – de forma automatizada ou não – mediante o consentimento de seu proprietário, certamente representará um grande avanço e exemplo não apenas no âmbito jurídico brasileiro, como também mundial.

No entanto, a complexidade quando se trata de regulamentação da proteção de dados fica evidente quando analisados casos concretos, como o recente surgimento de sites como o “Tudo sobre todos”, que permitia que o usuário pesquisasse a partir do nome de uma pessoa ou número do CPF uma gama de outras informações como data de nascimento, local de trabalho, endereços e nomes de parentes e vizinhos. Pois, conforme alegado pelo responsável do site, todas as informações disponíveis eram igualmente públicas, tendo sido coletadas de cartórios, processos judiciais, diários oficiais, redes sociais e consultas em sites públicos, portanto, o argumento em favor da sua legalidade seria de que o site apenas reunia dados públicos dispersos. (BIONI; RIBEIRO, 2015)

Neste sentido, mesmo que o Anteprojeto de Lei de Dados Pessoais represente um grande avanço para a regulamentação de dados pessoais, ainda existem algumas dificuldades no seu texto, como a exceção da necessidade do consentimento em relação a dados de acesso público irrestrito no artigo 11, visto que, há uma linha tênue entre o que é dado público e o que é dado público irrestrito. Logo, caso o texto permaneça inalterado certamente este artigo ocasionará uma insegurança jurídica.

Outro problema que também é encontrado no texto do Anteprojeto de Lei, é que parte-se do pressuposto que existem duas partes envolvidas: o cedente de dados e o cessionário, quando, na verdade, diante das novas capacidades tecnológicas de coleta, análise e processamento de dados, nem sempre existe um cedente.

> [...] em um contexto de análise e processamento de bases de dados extremamente volumosas nem sempre existe um cedente, além de que tal análise, por natureza, pode gerar resultados imprevisíveis. Assim, não seria razoável responsabilizar o criador da base de dados por possíveis ofensas aos titulares, e tal fato representaria um forte desincentivo para a inovação por meio de análise de *Big Data*. (CARLONI, 2013, p. 38)

Assim, percebe-se que a complexidade do problema ainda é a maior dificuldade para a criação de leis eficientes envolvendo a proteção de dados pessoais. Portanto, é fundamental para que as futuras leis tenham efeitos práticos satisfatórios para a sociedade, um entendimento prévio do legislador e dos operadores do direito a respeito das dificuldades e dos riscos enfrentados pela privacidade de dados pessoais na atual sociedade.

Não se pode negar que uma lei específica regulamentando a proteção de dados pessoais trará mais segurança e certeza aos julgamentos. Além disso, a existência de uma legislação específica sobre o tema pode contribuir para resolver o problema de que, atualmente, as informações de brasileiros armazenadas em serviços de e-mails, redes sociais, ferramentas de backup em nuvem, entre outros serviços baseados na internet, ficam sujeitas aos termos de uso definidos pelas empresas de tecnologia, que em sua maioria estão alinhados com as leis americanas, que por sua vez permitem a coleta de dados e de comunicações estrangeiras por órgãos de segurança do governo americano.

O interesse dos governos na coleta de dados através da internet tem se revelado um grande desafio em termos de proteção de dados pessoais e violação de privacidade no ambiente virtual. Dada sua natureza global e distribuída, a internet tornou-se um poderoso instrumento também para os governos que pretendem obter vantagens no cenário global.

Assim, na sociedade atual onde “informação é poder”, o Estado passa a ser um dos maiores interessados em obter o poder advindo dos mecanismos de vigilância em massa, transformando-se em uma das principais ameaças ao direito à privacidade. Portanto, a análise dos impactos da atual vigilância à privacidade dos cidadãos e a abordagem jurídica do tema requer um aprofundamento a respeito da vigilância praticada pelos governos.

2 VIGILÂNCIA GOVERNAMENTAL: CONFLITOS E DESAFIOS

A internet surgiu fazendo com que as pessoas acreditassem no seu poder de proporcionar comunicações muito mais livres de censura do que a grande mídia. No entanto, poucos atentaram para o fato de que com isso também vinha o poder de vigiar todas as comunicações (ASSANGE, 2013, p. 43). Poder este, que logo despertou o interesse dos governantes que passaram a investir intensamente em tecnologias de vigilância em massa.

Em junho de 2013, o jornal britânico *The Guardian* publicou os primeiros dados vazados por Edward Snowden, ex-funcionário da Agência de Segurança Nacional norte-americana (NSA), desvendando a vigilância ilimitada praticada pelo governo dos Estados Unidos. As revelações mostraram ao mundo detalhes de programas de vigilância eletrônica usados pelo governo americano capazes de acabar com a privacidade dos cidadãos em qualquer parte do mundo.

Segundo Glenn Greenwald, jornalista que iniciou a divulgação dos documentos vazados por Snowden no jornal britânico, a internet tornou-se um instrumento sem precedentes para a democratização, liberalização e até emancipação. Daí o interesse e ambição dos governos de “coletar tudo”. (GREENWALD, 2014, p. 181)

> Desde que começou a ser usada de forma ampla, a internet foi vista por muitos como detentora de um potencial extraordinário: o de libertar centenas de milhões de pessoas graças à democratização do discurso político e ao nivelamento entre indivíduos com diferentes graus de poder. A liberdade nas rede – a possibilidade de usá-la sem restrições institucionais, sem controle social ou estatal, e sem a onipresença do medo – é fundamental para que essa promessa se cumpra. Converter a internet em um sistema de vigilância, portanto, esvazia seu maior potencial. Pior ainda, a transforma em uma ferramenta de repressão, e ameaça desencadear a mais extrema e opressiva arma de intrusão estatal já vista na história da humanidade. (GREENWALD, 2014, p. 15 e 16)

Antes de tudo, para analisar aspectos da vigilância governamental, identificando desafios e limitações de sua regulamentação jurídica como se propõe o presente estudo, faz-se necessária, uma compreensão acerca da atual dimensão da vigilância. Para tanto, optou-se por iniciar a abordagem do assunto com uma breve

exposição sobre quatro formas de coleta de dados praticadas pelo governo norte-americano, com base nos relatórios divulgados por Snowden e publicados no livro “Sem Lugar Para Se Esconder” (2014), do jornalista Glenn Greenwald, quais sejam: coleta de dados diretamente de empresas de internet; interceptação de cabos de fibra óptica; colocação de *backdoors* em equipamentos; cooperação entre agências de inteligência.

A coleta de dados diretamente de empresas de internet foi revelada por Snowden, principalmente em documentos que fazem referência ao programa de vigilância denominado PRISM. Este programa permite à NSA coletar dados diretamente dos servidores de nove das maiores empresas da internet (Microsoft, Google, Facebook, Yahoo!, Apple, YouTube, AOL, Paltalk e Skype). Nos documentos vazados por Snowden, um slide de uma apresentação sobre o programa revela a capacidade da agência de coletar diversos tipos de dados dos usuários, como e-mails, vídeos, fotos, chamadas de voz, histórico de pesquisas, transferência de arquivos e quaisquer outros dados em poder destas empresas. Percebe-se que, embora as empresas listadas neguem, o programa PRISM é provavelmente executado com a participação das companhias, que fornecem para a NSA acesso direto aos seus servidores. Inclusive, alguns documentos revelam a data de ingresso de cada uma das companhias no programa. (GREENWALD, 2014, p. 114-119)

A interceptação de cabos de fibra óptica (por onde circulam a grande maioria do tráfego telefônico e da Internet) é outra forma de coleta de dados, conhecida por vigilância *Upstream* (termo usado pela NSA) que envolve a interceptação de cabos de fibra óptica e outros tipos de infraestrutura (de redes), com a colaboração de grandes empresas de telecomunicações no mundo todo. Esse tipo de coleta massiva de dados envolve diversos programas (FAIRVIEW, BLARNEY, STORMBREW, OAKSTAR) que se diferenciam geralmente pela fonte de dados (empresa de telecomunicação), pelos alvos da interceptação (países, organizações ou até mesmo chefes de Estado) e pela classificação do acesso às informações interceptadas (NSA, FBI, CIA, agências de inteligência de países parceiros). Um slide, revelado por Snowden e publicado pelo jornal *The Washigton Post*, possivelmente utilizado para treinar novos agentes, orienta o uso em conjunto do sistema *Upstream* (coleta a partir de cabos de fibra óptica) e do programa PRISM

(coleta direta nos servidores das empresas de internet). (GREENWALD, 2014, p. 108-114)

Alguns dos métodos da NSA são bastante invasivos e imorais, pois envolvem a colocação de *backdoors* (porta dos fundos) em equipamentos eletrônicos, que são recursos que permitem o acesso remoto aos sistemas ou à rede infectada.

> Um relatório de junho de 2010 do chefe do Departamento de Desenvolvimento de Acesso e Alvos da NSA é de uma clareza chocante. A agência recebe e intercepta, de forma rotineira, roteadores, servidores e outros equipamentos de rede que serão exportados pelos Estados Unidos antes que sejam despachados para os clientes internacionais. Ela então implanta ferramentas de vigilância do tipo porta dos fundos, reembala os produtos com um selo de fábrica e os despacha. Assim, a NSA consegue acesso a redes inteiras e aos seus usuários (GREENWALD, 2014, p. 156).

Os *backdoors*, que podem ser implantados tanto no hardware (equipamento físico) quanto no software (programas e sistemas operacionais), concedem acesso remoto a computadores e *smartphones* no mundo todo.

Por fim, outra forma de obtenção de informações da NSA envolve a cooperação com agências de inteligência de outros países. Esses países se relacionam com a agência americana em diferentes níveis de cooperação. No entanto, segundo os documentos revelados por Snowden, destaca-se a aliança formada por Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia – conhecida como os Cinco Olhos ou *Five Eyes* – e suas respectivas agências de inteligência, principais parceiras na formação de um sistema de vigilância e espionagem global. (GREENWALD, 2014, p. 126)

Percebe-se, portanto, que estas quatro formas de interceptação de dados (e não únicas) utilizadas pela NSA constituem um gigantesco sistema de rastreamento e controle invisível por parte do governo, representando um perigo potencial para o futuro, especialmente se sociedades totalitárias acabarem tendo acesso a estas tecnologias.

> Considerado em sua totalidade, o acervo de Snowden levava, em ultima instância, a uma conclusão bem simples: o governo dos Estados Unidos construíra um sistema cujo objetivo é a completa eliminação da privacidade eletrônica no mundo inteiro. Longe de ser uma hipérbole, esse é o objetivo literal e explicitamente declarado do Estado de vigilância: coletar, armazenar, monitorar e analisar todas as comunicações eletrônicas de todas as pessoas ao redor do mundo (GREENWALD, 2014, p. 101).

Contudo, não se deve supor que as atividades de monitoramento são uma exclusividade dos Estados Unidos. Embora as revelações feitas por Edward Snowden digam respeito ao incrível poder de vigilância do governo americano, a abrangência do monitoramento ultrapassa em muito os limites do vazamento de Snowden.

> Já ficou evidente que a China, Inglaterra, Israel, Austrália, Nova Zelândia, Canadá, França, Rússia e a maioria dos regimes estáveis do Oriente Médio têm programas similares, e a tendência é que isso aumente nos próximos anos, com a redução constante no custo dos equipamentos e o incremento no uso das comunicações, principalmente pela Internet. A caixa de Pandora foi aberta, e não se tem notícia de nenhuma vez em que os males tenham voltado novamente para dentro dela. (BERG, 2015)

As revelações de Edward Snowden perturbaram o modo de funcionamento dos sistemas de vigilância com a divulgação de sua existência. Pela primeira vez, as pessoas tomaram conhecimento da verdadeira capacidade da vigilância atual, sendo que, diversos países descobriram serem vítimas da vigilância norte-americana, o que provocou um intenso debate mundial.

De acordo com os relatórios divulgados por Snowden, mais de 30 chefes de Estado haviam sido vigiados pela NSA, incluindo a presidente brasileira Dilma Rousseff e a chanceler alemã Angela Merkel, que tiveram suas ligações telefônicas e por e-mail espionadas (SENADO FEDERAL, 2014, p. 12). Mas como a NSA consegue rastrear as ligações de Angela Merkel e Dilma? Possivelmente através do uso de *backdoors* nos telefones celulares, pois equipamentos como *smartphones*, que permanecem conectados diretamente na rede, são alvos fáceis de monitoramento quando infectados.

> [...] já reparou que a maioria dos programas instalados solicitam acesso à rede, agenda, lista de chamadas e dados de posicionamento, mesmo quando são jogos ou aplicativos que não precisariam dessas informações? Pois é dessa forma que a NSA consegue dados de ligações ao redor do mundo, mesmo em países onde ela não possui monitoramento. Provavelmente foi assim que as ligações da Angela Merkel e da Dilma foram rastreadas, e provavelmente as suas também estão sendo. (BERG, 2013)

Ainda em 2012, antes do caso Snowden, o governo alemão já havia alertado suas principais entidades para não utilizar o programa *Windows 8* da *Microsoft* em seus computadores. Segundo documentos internos vazados do Escritório Federal Alemão de Segurança da Informação (BSI), que o site *Die Zeit* obteve, especialistas

em TI da Alemanha descobriram que o sistema operacional da *Microsoft* é completamente perigoso para a segurança de dados do computador, pois permite que a empresa possa controlar o seu computador remotamente através de um *backdoor*. Logo, a NSA tendo acesso às chaves para acessar o *backdoor* poderia espionar qualquer equipamento com este sistema operacional (RICHTER, 2013).

Segundo Paulo Pagliusi, referência nacional em Segurança da Informação, o Brasil tem sido um alvo constante de espionagem e sua situação atual é preocupante. Exemplo disso, é que documentos revelaram também a espionagem de grandes empresas de energia brasileira como a Petrobras e a Eletrobrás.

> Vivemos um momento simplesmente estarrecedor. Segundo o material coletado por Edward Snowden que observei, o Brasil é alvo prioritário das agências governamentais de espionagem conhecidas como “Five Eyes” (EUA, Reino Unido, Canadá, Austrália, Nova Zelândia). Há acesso generalizado pela “porta dos fundos” (backdoors) a servidores de empresas operadoras da Internet, monitorando redes e comunicações online com tecnologia bem avançada (PAGLIUSI, 2014).

Nota-se, pois, que o astronômico sistema de vigilância desenvolvido pelos Estados Unidos para manter sua hegemonia e controle sobre o mundo apresenta diversos perigos relacionados ao seu uso, que vão muito além de manipulação diplomática ou de obtenção de vantagens econômicas.

> Quando o país consegue saber tudo o que todos estão fazendo, dizendo, pensando e planejando – seus próprios cidadãos, populações estrangeiras, corporações internacionais, líderes de outros governos –, seu poder sobre eles é maximizado. Isso é duplamente verdadeiro quando o governo opera em níveis de sigilo cada vez mais altos. O sigilo cria um espelho de apenas uma direção: o governo dos Estados Unidos vê tudo o que o resto do mundo faz, inclusive, sua própria população, mas ninguém sabe de suas ações. É o cúmulo do desequilíbrio, que dá lugar a mais perigosa de todas as condições humanas: o exercício de um poder ilimitado sem transparência nem prestação de contas (GREENWALD, 2014, p.181).

Portanto, os grandes investimentos em vigilância verificados principalmente nos Estados Unidos e em países europeus com a justificativa da necessidade de combate ao terrorismo e à violência ampliaram o poder de controle dos governos e despertaram uma preocupante tendência no sentido de flexibilizar direitos fundamentais em favor da segurança pública. Dessa forma, a realidade chocante exposta por Snowden revelou também a premente necessidade de repensar o equilíbrio entre o direito à privacidade e a defesa da segurança pública.

2.1 Conflito entre a defesa da segurança pública e direito fundamental à privacidade

Como já visto, em grande medida os mecanismos de vigilância eletrônica foram construídos ou ampliados sob a justificativa da necessidade de ampliação da segurança pública após os atentados de 11 de setembro de 2001. No entanto, vale lembrar que, anteriormente aos atentados, um conjunto de direitos fundamentais de defesa relativamente ao tratamento informático de dados pessoais estava ganhando terreno. O poder fascinante, mas ameaçador, das novas tecnologias levara a um aumento de leis dando maior autonomia ao direito à autodeterminação informativa, pretendendo assim, impedir que o homem se transformasse em um “simples objeto de informações”. (CASTRO, 2003, p. 01)

Se por um lado, a evolução tecnológica aumentou a preocupação com a preservação de direitos fundamentais, aumentou também as capacidades de vigilância e defesa da segurança pública dos governos. Assim, estabeleceu-se um conflito constante entre os direitos à privacidade e à segurança. De modo que, as restrições que a um e a outro se imponha estabelecer, são realizadas em nome da necessidade de defesa de outro direito constitucionalmente estabelecido, conforme argumenta Catarina Sarmento e Castro.

> Trata-se de encontrar o equilíbrio entre o direito à autodeterminação informativa e o direito à segurança, o que não deixa de ser a procura da harmonia entre a liberdade individual (neste caso, essencialmente informática) e a segurança: a primeira, sem a segunda, gera o caos e a anarquia, a segunda, sem a primeira, conduzirá à construção de Estados totalitários. (CASTRO, 2003, p. 24)

Desse modo, o conflito entre direitos que se estabelece origina o seguinte questionamento: até que ponto pode o governo intrometer-se na vida dos cidadãos alegando estar perseguindo um bem maior, como a segurança da nação? A resposta a essa pergunta é invariavelmente motivo de polêmica e grandes discussões no mundo todo.

Inicialmente, é preciso analisar as posições conflitantes, sendo que, há aqueles que defendem que a segurança de um país é o bem maior a ser protegido, enquanto há outros que criticam fortemente as práticas de vigilância. Dentre os que se encaixam na primeira forma de pensar, está o general Keith Alexander, diretor da NSA, que saiu em defesa dos sistemas de vigilância, alegando que o futuro dos EUA dependia da habilidade de defesa contra ataques cibernéticos e ameaças terroristas. O próprio presidente Barack Obama por algumas vezes argumentou que o mundo é atualmente "mais estável" por causa das ações americanas na política internacional, embora tenha se comprometido a fazer uma revisão das práticas da NSA. (UCHOA, 2013)

Sabe-se, pois, que a vigilância é muito útil para governos e instituições na aplicação da lei e para manter a fiscalização e segurança. Especialmente na atualidade em que a vigilância não se resume apenas em monitorar através de uma câmera de vídeo, mas sim a utilização de uma série de tecnologias que permitem reconhecer e monitorar as ameaças, impedindo e investigando atividades criminosas.

> Extremamente vinculada ao tema da violência e da segurança, a vigilância tem se mostrado com uma espécie de solução natural ao quadro de desordem e medo que se instaura nas grandes cidades contemporâneas. Parece que a vigilância se tornou um meio privilegiado de reação e principalmente de prevenção, não só por parte de iniciativas privadas, mas também por parte do poder público. (CASTRO, 2008, p. 37)

Neste sentido, Paesani (2012, p. 41) ressalta que a crescente escalada da violência tem possibilitado, ao Poder Público, a captação de informações e dados privados, sacrificando-se os direitos individuais em prol do bem comum. Sendo que a doutrina e o sistema jurídico têm legitimado essas interferências em função de que cabe ao Estado conceder segurança a seus cidadãos.

Uma maneira de tentar resolver o conflito entre os direitos à segurança pública e à privacidade é através da teoria da ponderação, de Alexy, que faz referência ao conflito entre princípios, em que se deve analisar qual princípio é mais adequado para ser aplicado àquele caso concreto, sempre tendo em mente as conseqüências da não aplicação do princípio que será deixado de lado. Através da análise de decisões em casos concretos, Alexy procura explicar racionalmente o a

ponderação em sentido específico, verificando se a importância da satisfação de um direito fundamental justifica a não satisfação do outro.

> Essa relação de tensão não pode ser solucionada com base em uma precedência absoluta de um desses deveres, ou seja, nenhum desses deveres goza, “por si só, de prioridade”. O “conflito” deve, ao contrário, ser resolvido “por meios e um sopesamento entre os interesses conflitantes”. O objetivo desse sopesamento é definir qual dos interesses – que abstratamente estão no mesmo nível – tem maior peso no caso concreto: “Se esse sopesamento levar à conclusão de que os interesses do acusado, que se opõem à intervenção, têm, no caso concreto, um peso sensivelmente maior que os interesses em que se baseia a ação estatal, então, a intervenção estatal viola o princípio da proporcionalidade e, com isso, o direito fundamental do acusado [...]. (ALEXY, 2008, p. 95)

Pode-se considerar que os defensores dos sistemas de vigilância, através de ponderações, elegeram a defesa da segurança como um interesse que deve sobrepor-se ao direito à privacidade, apesar das más conseqüências que podem advir de uma atuação tão direta do Estado na vida dos cidadãos. Esse entendimento também encontra fundamento no princípio utilitarista, segundo o qual uma ação que promova mais benefícios que malefícios à sociedade – como a prevenção contra ataques terroristas – pode ser efetivada mesmo que contrarie direitos considerados fundamentais. Segundo o filósofo Jeremy Bentham, fundador da doutrina utilitarista, todo argumento deve implicitamente inspirar-se na idéia de maximizar a felicidade (SANDEL, 2012, p. 48). Neste caso, a prevenção de milhares de mortes representaria uma felicidade maior do que os cidadãos não terem suas comunicações e dados pessoais coletados, justificando assim, a sobreposição da segurança em relação à privacidade.

Por outro lado, em um modelo de vigilância absoluta é de se esperar que existam abusos e discriminações. Como bem analisado por Michel Foucault ao comentar a relação entre dispositivos disciplinares e esquemas de exclusão.

> Atrás dos dispositivos disciplinares se lê o terror dos “contágios”, da peste, das revoltas, dos crimes, da vagabundagem, das deserções, das pessoas que aparecem e desaparecem, vivem e morrem na desordem (FOUCAULT, 1987, p. 164)

Percebe-se, portanto, que quando os dados privados dos cidadãos são sistematicamente coletados e explorados por governos em nome da segurança coloca-se em risco uma série de liberdades civis e políticas. Uma vigilância poderosa

não é apenas um instrumento para promover a segurança pública, mas também uma eficiente ferramenta para controlar a dissidência política e prática de censura, podendo inclusive representar uma grave ameaça à democracia. Dessa forma, manifestantes, ativistas ou quaisquer cidadãos contrários ao governo não precisam cometer nenhum crime para serem perseguidos, basta enviarem mensagens, e-mails ou ligarem para outras pessoas com a intenção de protestar.

Conforme Flávia Piovesan, políticas de segurança máxima como a adotada pelos Estados Unidos representam enormes riscos aos direitos, liberdades e garantias fundamentais.

> No cenário do Pós 11 de setembro o risco é que a luta contra o terror comprometa o aparato civilizatório de direitos, liberdades e garantias, sob o clamor de segurança máxima. Basta atentar à doutrina de segurança adotada nos EUA pautada: a) no unilateralismo; b) nos ataques preventivos e c) na hegemonia do poderia militar norte-americano. Atente-se às nefastas conseqüências para a ordem internacional se cada um dos duzentos Estados que integram a ordem internacional invocasse para si o direito de cometer "ataques preventivos", com base no unilateralismo. Seria lançar o próprio atestado de óbito do Direito Internacional, celebrando o mais puro hobbesiano "Estado da Natureza", em que a guerra é o termo forte e a paz se limita a ser a ausência da guerra. A escusa de combater o chamado "império do mal" tem propagado, sobretudo, o "mal do império". (PIOVESAN, 2006, p. 24)

Neste sentido, Julian Assange, editor-chefe do *WikiLeaks* – organização que se dedica a publicar documentos secretos revelando a má conduta de governos, empresas e instituições – argumenta que a própria consciência de vigilância tem desencorajado muito a população – não o fato de eles estarem sendo censurados, mas o de saber que tudo o que lêem é monitorado e registrado. "A consciência da vigilância é algo que muda o comportamento das pessoas fazendo-as desanimar e desistir de protestar contra vários tipos de autoridade." (ASSANGE, 2013, p. 123).

Outro ponto a ser destacado, é que o desenvolvimento de poderosos sistemas de vigilância vem ocorrendo em silêncio no mundo todo. O desconhecimento desta realidade pela sociedade, aliado ao encantamento com novas tecnologias que cada vez mais promovem a renúncia à própria intimidade acabaram por gerar, em parte da população, reações de incompreensão ou de pura indiferença quanto às violações de direitos.

> Tal postura é, a princípio, fruto da imensa dificuldade em compreender em que de fato implicam as novas tecnologias, agravada pela consciência de

> que sabê-lo pode não ser de grande ajuda, frente à escassez de meios para controlá-las. Todo este processo, ao mesmo tempo, pode ser entendido como parte de uma tentativa de neutralização do impacto tecnológico, que visaria a uma lenta absorção desta realidade pela sociedade, pela qual a privacidade contaria menos, o que seria ao fim admitido como uma "conseqüência natural" – um fato da vida, induzido pela valorização de determinados valores da sociedade de consumo. Em tal processo não conta pouco o que Denninger chamou de "explosão de ignorância": o fato que uma abundância de informações típica da pós-modernidade acaba por se traduzir em menos conhecimento. (DONEDA, 2006, p. 12)

A evolução tecnológica e contexto social de combate ao terrorismo e a violência dos últimos anos fizeram com que a segurança pública prevalecesse quando confrontada com o direito à privacidade. No entanto, esse panorama social tende a modificar-se na medida em que as pessoas adquiram consciência desse desequilíbrio entre direitos e dos perigos que ele representa.

Nesse ponto, pode-se concluir que uma resposta adequada para o questionamento levantado no início deste tópico seria de que a vigilância, especialmente a praticada em sigilo e indiscriminadamente pelo Estado, não legitima a violação do direito à privacidade, e que, portanto, é imprescindível que a sociedade encontre rapidamente uma maneira de harmonizar os direitos em conflito.

Portanto, para se chegar ao equilíbrio/harmonia entre direitos tão importantes na Era da Vigilância é fundamental que a partir de projeções entre as promessas e perigos das novas tecnologias seja conferido um mínimo de regulamentação jurídica capaz de oferecer transparência e controle público acerca da utilização das tecnologias de vigilância, assim como mecanismos de responsabilização e reparação por danos ocasionados em virtude do tratamento de dados coletados.

> O equilíbrio apenas será atingido quando o uso dos mecanismos – potenciadores da segurança, mas invasores das trevas a que cada um tem direito – puder, ele mesmo, ser transparente, submetendo-se a sua utilização ao controle público. [...] Não deverá ser afastada, seja em que circunstância for, a possibilidade de recurso a mecanismos de tutela independente, designadamente jurisdicional, que possam ser utilizados pelo indivíduo sempre que considere violados os seus direitos digitais. A esta garantia deve andar associado o direito à reparação pelos danos que este possa sofrer em virtude de tratamentos de dados ilícitos. [...] São também indispensáveis normas claras que disciplinem a utilização destes mecanismos de vigilância. Funcionando essencialmente como normas de conduta procedimental, o seu papel será também o de tornar públicas as condições da realização destes tratamentos de dados. (CASTRO, 2003, p. 25)

Passados dois anos das primeiras revelações de Snowden, percebe-se uma mudança de consciência global acerca da importância da privacidade e dos perigos da vigilância em massa em diversos países, seja através do debate para elaboração de leis mais eficientes para a proteção de dados pessoais, seja por decisões judiciais considerando ilegais algumas formas de interceptações de dados praticadas por governos.

Segundo a Anistia Internacional – organização não governamental que defende os direitos humanos – um dos principais reflexos das revelações feitas por Edward Snowden é que, atualmente, sabe-se muito mais sobre o que os governos fazem. E ao adquirir maior consciência, a opinião pública reagiu com uma enorme oposição à vigilância em massa praticada pelos governos.

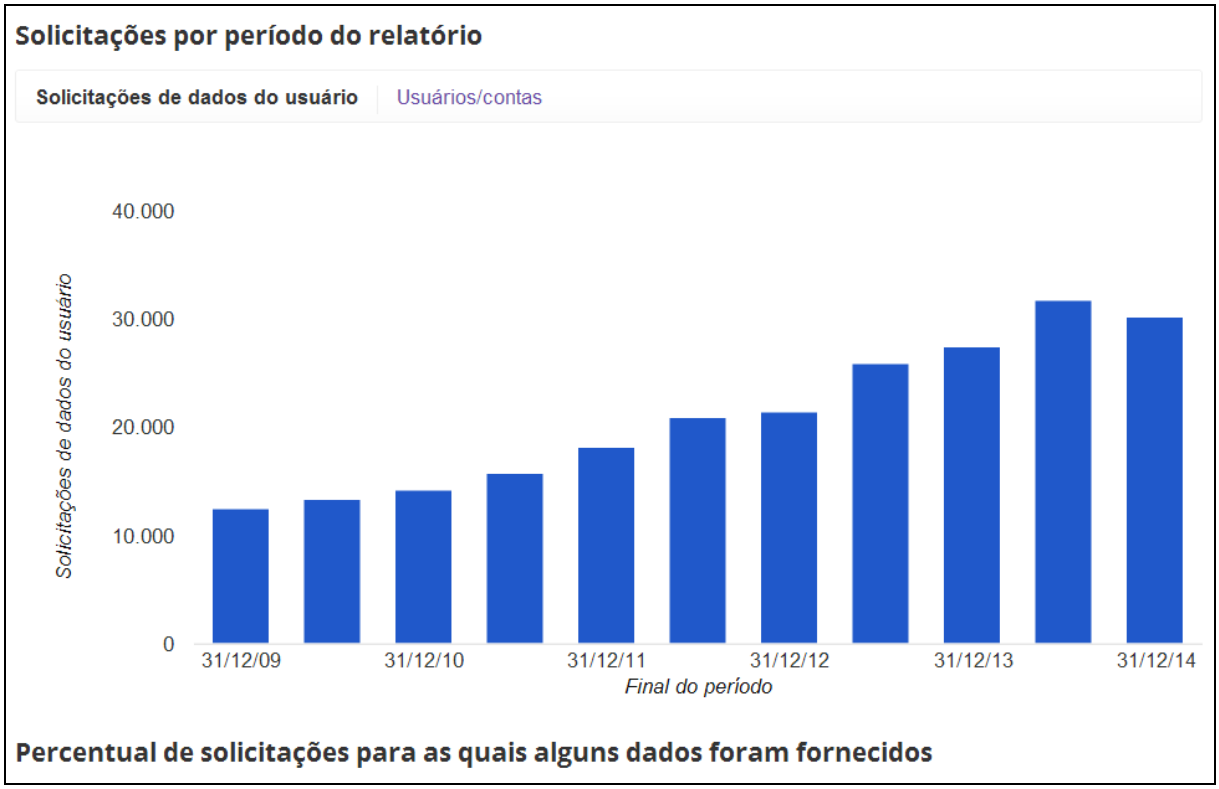
> Na pesquisa que realizamos em 13 países de todos os continentes, descobrimos que 71% das pessoas se opõem firmemente a que seus governos espionem a comunicação telefônica e por internet. Mais de 450 organizações e especialistas de todo o mundo subscreveram alguns princípios “necessários e proporcionais” para aplicar os direitos humanos à vigilância das comunicações. Finalmente, mais de 80.000 pessoas assinaram a petição da Anistia Internacional no mundo todo para que a vigilância em massa seja proibida (ANISTIA INTERNACIONAL, 2015).

A reação negativa da opinião pública diante dos “escândalos da vigilância” fez com que as empresas de tecnologia fossem bastante afetadas. Analistas do mundo todo estimaram que por causa da suspeita dos consumidores de tecnologia, especialmente as empresas de computação em nuvem, perderiam bilhões de dólares em serviços de internet (REGALADO, 2014). Isto ocasionou uma mudança de postura nas empresas da internet que passaram a incorporar elementos de proteção à privacidade nos seus produtos e serviços. “Várias grandes empresas, entre elas a *Apple*, *Google* e *Whatsapp*, aumentaram a segurança e a criptografia básicas que oferecem a seus clientes.” (ANISTIA INTERNACIONAL, 2015)

Outro aspecto da mudança de comportamento de empresas da internet foi uma maior oferta de transparência com relação ao compartilhamento de dados com órgãos governamentais. Recentemente, o Google passou a divulgar relatórios com o número de solicitações de governos do mundo todo a respeito de dados dos usuários de seus serviços. No gráfico divulgado contendo o número total de solicitações de governos (Figura 1), embora não se possa mensurar a confiabilidade, percebe-se uma leve redução de solicitações no último período apresentado

(segundo semestre de 2014), possivelmente reflexo da opinião pública com relação ao tratamento de dados pessoais, após as revelações de Snowden.

Figura 1 – Gráfico com o total de solicitações governamentais de países a respeito de dados de usuários.



Fonte: Google Transparency Report

No início de 2015, grande empresas de tecnologia como *Google*, *Apple*, *Microsoft, Facebook, Yahoo* e *Twitter* criaram uma coalizão para exigirem uma reforma na política de vigilância dos EUA e mais transparência dos órgãos públicos. Estas empresas estão se unindo a grupos da sociedade civil e a associações comerciais para estimular os legisladores a assegurar uma maior transparência e prestação de contas em torno de programas de vigilância e pressionar o Congresso dos EUA para acabar com a coleta em massa de metadados de comunicações digitais entre americanos por agências do governo, como a NSA (O GLOBO, 2015).

A consciência dos perigos dos atuais sistemas de vigilância e o aumento da preocupação com a preservação de direitos fundamentais influenciaram diversos

países a buscar um controle mais estreito em leis que regulamentam a proteção de dados pessoais. No Brasil, os esforços dos cidadãos levaram ao Marco Civil, a primeira lei de direitos na internet do mundo, e atualmente se debate a criação da Lei de Proteção de Dados Pessoais.

Desde o dia 1º de junho de 2015, o *Patriot Act* – legislação vigente que permitia a interceptação de ligações telefônicas e mensagens eletrônicas sem prévia autorização judicial por órgãos de segurança – expirou, sendo rejeitada sua extensão. Diante disso, o Senado dos Estados Unidos aprovou um projeto de lei que muda o controverso programa de coleta de dados e telefones da NSA. A lei, conhecida como *USA Freedom Act* (Lei da Liberdade dos EUA), determina que essa coleta de dados de cidadãos americanos só pode ser feita com decisões judiciais individuais. Ou seja, o texto não acaba com o programa de espionagem, mas limita consideravelmente o poder das agências. O presidente dos EUA, Barack Obama anunciou, que pretende sancionar a lei, pois ela protege as liberdades civis e a segurança nacional. (ÉPOCA, 2015)

Contudo, não se deve esquecer que os governos pouco têm feito no sentido de desfazer os programas de vigilância. Pelo contrário, muitos países correm para ampliar suas capacidades. Dessa forma, o direito à privacidade permanece sob a ameaça da poderosa vigilância governamental. E cada vitória em defesa deste direito deve ser muito comemorada para aumentar a percepção de sua importância social, conforme salienta o próprio Edward Snowden.

> No entanto, o equilíbrio de poder está começando a mudar. Estamos testemunhando o surgimento de uma geração pós-terror, uma geração que rejeita uma visão de mundo definida por uma tragédia singular. Pela primeira vez desde os ataques de 11 de setembro, vemos o esboço de uma política que se afasta da reação de medo em favor da resiliência e da razão. Com cada vitória judicial, com cada mudança na lei, demonstramos que os fatos são mais convincentes do que o medo. E, como uma sociedade, nós redescobrimos que o valor de um direito não está naquilo que ele esconde, mas sim no que ele protege. (SNOWDEN, 2015)

Nesta perspectiva, parecem promissoras as leis elaboradas com o intuito de proteção de dados pessoais visando dar aos cidadãos não apenas o controle dos seus dados pessoais, mas também estabelecendo a necessidade de consentimento para o fluxo de informações, independentemente se o dado é público ou privado. Contudo, deve-se ter consciência de que, diante de uma espionagem na qual a privacidade de uma pessoa é violada de maneira sigilosa, auxiliada pela facilidade

na obtenção de informações com a utilização das novas tecnologias, esperar que o direito por si só seja suficiente para impedir a violação de direitos fundamentais pode ser inviável.

2.2 Limites da regulamentação e soluções na era da vigilância

Atualmente, o avanço tecnológico ocorre tão depressa e com consequências tão profundas, que as formas de regulação do direito não conseguem acompanhá-lo. As próprias atividades das empresas de vigilância são cada vez mais difíceis de discernir e, consequentemente, uma perspectiva jurídica de tais atividades torna-se um enorme desafio, como explica Siva Vaidhyanathan em relação ao Google:

> Em algumas áreas, o Google talvez seja regulamentado muito ligeiramente. Em outras, talvez o seja excessiva ou inadequadamente. Não há uma noção geral de regulamentação que se possa aplicar a uma empresa tão complexa, envolvida em tantas áreas distintas da vida e do comércio. (VAIDHYANATHAN, 2011, p.61)

Desse modo, é preciso que o Direito acompanhe os avanços da sociedade, renovando-se a cada dia para que não fique ultrapassado, principalmente no que tange aos direitos humanos fundamentais e em relação às novas tecnologias que se modificam e evoluem com enorme frequência.

Além disso, na sociedade moderna, permeada pela vigilância de governos, verifica-se a importância da discussão em torno da relevância jurídica e das consequências da coleta massiva de dados, especialmente em um contexto em que a informação assume papel de destaque no jogo do poder, conforme alertado por Assange.

> [...] assim como o controle sobre o petróleo orienta a geopolítica global e é sinônimo de poder, o mesmo acontece com os cabos de fibra óptica que transmitem dados de milhões de inocentes e representam a grande alavanca no jogo geopolítico (ASSANGE, 2013, p. 20).

Considera-se, que em uma sociedade ideal as tecnologias de vigilância deveriam ser utilizadas com força suficiente para evitar resistências ilegais (crimes, terrorismo, guerra civil), mas não a ponto de possibilitar um estado totalitário. Dessa

maneira, conforme o quadro (Quadro 2) desenvolvido por David Brin no livro *The transparent society*, e analisado por Vianna (2006, p. 164), é possível cogitarmos quatro perspectivas para o futuro com base na transparência da vigilância exercida sobre os cidadãos e sobre os governos.

	O CIDADÃO É VIGIADO	**O CIDADÃO NÃO É VIGIADO**
O CIDADÃO VIGIA	**1º CENÁRIO** Prováveis tecnologias possibilitam aos cidadãos exigirem uma prestação de contas do poder; Prováveis tecnologias possibilitam ao poder exigir uma prestação de contas dos cidadãos.	**2º CENÁRIO** Prováveis tecnologias possibilitam aos cidadãos exigirem uma prestação de contas do poder; Prováveis tecnologias obstruem o poder de exigir uma prestação de contas dos cidadãos.
O CIDADÃO NÃO VIGIA	**3º CENÁRIO** Prováveis tecnologias impedem os cidadãos de exigirem uma prestação de contas do poder; Prováveis tecnologias possibilitam ao poder exigir uma prestação de contas dos cidadãos.	**4º CENÁRIO** Prováveis tecnologias impedem os cidadãos de exigirem uma prestação de contas do poder; Prováveis tecnologias obstruem o poder de exigir uma prestação de contas dos cidadãos.

Quadro 2 – Cenários hipotéticos para futuras civilizações tecnológicas. (Vianna, 2006, p. 146).

Atualmente, o momento vivido pela sociedade na Era da Vigilância se aproxima mais ao 3º cenário, no qual o poder vigia o cidadão e o cidadão muito pouco vigia o poder. No entanto, o cenário tende a mudar do n° 3 para o n° 1 na medida em que a sociedade passa a valorizar o direito à privacidade e a transparência na coleta e tratamento de dados por governos e empresas.

Segundo Vianna (2006, p. 148-150), David Brin conclui que o cenário ideal para uma sociedade futura é o cenário nº 1, no qual as pessoas são vigiadas pelo Estado, mas em contrapartida também o vigia, mantendo assim, um hipotético equilíbrio de forças. Neste cenário, a vigilância recíproca é perfeitamente aceitável. Assim, se alguma empresa desejasse coletar dados pessoais de consumidores, por exemplo, poderia fazê-lo somente se os diretores principais da empresa publicassem exatamente as mesmas informações, sobre si mesmos e suas famílias.

Contudo, segundo o autor, Brin não percebeu que os mecanismos de controle não estão concentrados nas mãos de quem detém o capital, mas de quem detém a informação que é o capital do século XXI e, portanto, não há transparência, ainda que esta seja um ideal a ser alcançado no que diz respeito aos governantes.

A poderosa vigilância dos governos veio para ficar. Tal constatação dá origem a duas outras afirmações. A primeira, é que cada vez mais as pessoas terão que tomar medidas específicas para proteger a própria privacidade, utilizando inclusive a própria tecnologia a seu favor. E a segunda, é que juristas e políticos devem se preocupar urgentemente em produzir leis capazes de conferir uma proteção abrangente aos aspectos derivados da coleta e tratamento de dados pessoais, a fim de, preservar o direito à privacidade.

Do ponto de vista jurídico, regulamentar a proteção de dados na sociedade moderna – em que as informações viajam ao redor do mundo através de redes sem fronteiras, em que dados podem acabar em países com leis diferentes de diferentes graus de força ou até mesmo nenhuma lei – seja talvez a maior dificuldade para a defesa da privacidade. Ademais, existe certo grau de indeterminação em qualquer tentativa de regulamentação pelo direito acerca do uso de tecnologias, o que segundo Doneda pode implicar em reconhecer-se a insuficiência do direito tradicional em determinadas ocasiões.

> Esta tarefa deve ainda projetar-se em uma conscientização sobre seus efeitos, chegando à reflexão sobre o papel do ordenamento jurídico na promoção e defesa de seus valores fundamentais, em um cenário em boa parte determinado justamente pela tecnologia – o que pode implicar em reconhecer a insuficiência da dogmática tradicional para tal fim. Esta dificuldade, traduzida em desafio, pode transformar-se em estopim para a tarefa de aproximar o ordenamento jurídico de um novo perfil da personalidade em uma sociedade que muda com velocidade, na qual os centros de poder e o espaço para a atuação do direito na regulação social são menos claros. (DONEDA, 2006, p. 25)

No âmbito global, o direito à privacidade encontra-se articulado em todos os principais instrumentos internacionais e regionais de direitos humanos, como por exemplo, na Declaração Universal dos Direitos do Homem (DUDH) de 1948, no artigo 12:

> Ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem ataques à sua honra e

> reputação. Contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei (UNESCO, 1998).

Segundo Flávia Piovesan, um dos grandes desafios para a efetiva regulamentação de direitos humanos é a construção de um Estado de Direito Internacional.

> Por fim, cabe enfatizar que, no contexto Pós 11 de setembro, emerge o desafio de prosseguir no esforço de construção de um “Estado de Direito Internacional”, em uma arena que está por privilegiar o “Estado Polícia” no campo internacional, fundamentalmente guiado pelo lema da força e segurança internacional.
> Contra o risco do terrorismo de Estado e do enfrentamento do terror, com instrumentos do próprio terror, só resta uma via – a via construtiva de consolidação dos delineamentos de um “Estado de Direito” no plano internacional. Só haverá um efetivo Estado de Direito Internacional sob o primado da legalidade, com o “império do Direito”, com o poder da palavra e a legitimidade do consenso.
> À luz deste cenário, marcado pelo poderio de uma única superpotência mundial, o equilíbrio da ordem internacional exigirá o avivamento do multilateralismo e o fortalecimento da sociedade civil internacional, a partir de um solidarismo cosmopolita. (PIOVESAN, 2006, p. 25)

Em que pese, atualmente, mais de 100 países tenham alguma forma de lei de privacidade e proteção de dados, é muito comum que a vigilância seja implementada sem levar em conta essas proteções nacionais (PRIVACY INTERNATIONAL, [2015?]). Este dado reforça a necessidade do diálogo internacional e de possíveis tratados como uma das possíveis formas para limitar o poder de vigilância dos Estados.

Segundo o advogado especialista em direitos civis, Alexander Abdo, em entrevista para o portal R7, um tratado internacional poderá ser uma das melhores ferramentas para controlar os abusos de vigilância entre governos. Abdo ainda se declarou favorável a uma mobilização global por meio da ONU, pois os cidadãos americanos aparentemente "não se importam tanto com os abusos" de espionagem, já que os recursos miram estrangeiros ou aqueles que estão envolvidos com atividades ilegais. (CERVONE, 2013)

Portanto, o Direito Internacional Público tem um papel fundamental em possibilitar a responsabilização do Estado violador de possíveis tratados internacionais.

> A evolução do Direito Internacional Público pode ser observada no próprio instituto da responsabilidade Internacional. A responsabilidade internacional

> do Estado refere-se às novas relações jurídicas que surgem quando um Estado, através de ação ou omissão, viola o comando de uma norma internacional em vigor.
> A responsabilidade se apresenta como ponto nuclear de todo sistema jurídico, para o qual convergem a natureza e o alcance das obrigações e a determinação das conseqüências jurídicas de sua violação. Todo ramo jurídico apresenta regras concernentes à responsabilização dos indivíduos que não observam as condutas prescritas, e assim não poderia ser diferente em relação à atuação internacional do Estado. (RAMOS; COSTA, [2012?], p. 3)

Os governos do Brasil e da Alemanha assumiram a dianteira das tratativas internacionais ao apresentar à Assembleia Geral da ONU projeto de resolução acerca do direito à privacidade na era digital. O texto divulgado pelo Ministério das Relações Exteriores na nota de imprensa nº 376 (BRASIL, 2013) merece alguns destaques:

> A Assembleia Geral,
>
> [...]
>
> PP8. Enfatizando que **a vigilância ilegal das comunicações, sua interceptação, bem como a coleta ilegal de dados pessoais constituem atos altamente intrusivos que violam o direito à privacidade** e à liberdade de expressão e que podem ameaçar os fundamentos de uma sociedade democrática, **(grifo nosso)**
>
> [...]
>
> 4. Conclama os Estados a:
>
> (a) respeitarem e protegerem os direitos referidos no parágrafo 1 acima, inclusive no contexto das comunicações digitais;
>
> (b) adotarem medidas com vistas à cessação das violações de tais direitos e a criarem condições para a prevenção de tais violações, inclusive assegurando que a legislação nacional relevante esteja em conformidade com suas obrigações no âmbito do direito internacional dos direitos humanos;
>
> (c) **revisarem seus procedimentos, práticas e legislação no que tange à vigilância das comunicações, sua interceptação e coleta de dados pessoais, inclusive a vigilância, interceptação e coleta em massa, com vistas a assegurar o direito à privacidade** e garantir a plena e eficaz implementação de todas suas obrigações no âmbito do direito internacional dos direitos humanos; **(grifo nosso)**
>
> (d) estabelecerem mecanismos nacionais independentes de supervisão, capazes de **assegurar a transparência do Estado e sua responsabilização em atividades relacionadas à vigilância das comunicações, sua interceptação e coleta de dados pessoais**; **(grifo nosso)**
> [...]

Percebe-se, que a resolução entre Alemanha e Brasil é clara ao considerar a vigilância em massa, bem como a interceptação e coleta indiscriminada de dados pessoais, uma forte afronta ao direito à privacidade. Além dessas reações contundentes – de países que tiveram seus principais governantes afetados diretamente pela espionagem – o aumento dos debates acerca da vigilância governamental contribuiu para o surgimento de uma série de propostas de reformas visando combater ou minimizar essas práticas.

Em se tratando de soluções para combater a vigilância em massa pode-se considerar duas abordagens distintas: A primeira utiliza da própria tecnologia para construção de dispositivos que impeçam a interceptação ou permitam o anonimato na internet. A segunda aplica controles democráticos por meio de leis para garantir o direito das pessoas ou forçar a prestação de contas.

Com relação à abordagem baseada na própria tecnologia, tem ganhado força a maior utilização de mecanismos de proteção de dados como a criptografia, que consiste basicamente em codificar informações de forma que o conteúdo criptografado somente possa ser lido pelo emissor e pelo destinatário (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p. 67). Inclusive, uma das recomendações em relação à segurança das comunicações apontadas pelo relatório final da CPI da Espionagem – que apurou denúncias de espionagem estrangeira no Brasil – consistia em ações no universo das tecnologias que desenvolvam algoritmos nacionais de criptografia. (SENADO FEDERAL, 2014, p. 60)

Tendo em vista que a centralização do sistema de gestão da internet mundial nos Estados Unidos, uma das possíveis reformas envolveria a construção de novas redes de comunicações.

> Não é segredo algum que, na Internet, todos os caminhos que vão e vêm da América Latina passam pelos Estados Unidos. A infraestrutura da internet direciona a maior parte do tráfego que entra e sai da América do Sul por linhas de fibra óptica que cruzam fisicamente as fronteiras dos Estados Unidos. O governo norte-americano tem violado sem nenhum escrúpulo as próprias leis para mobilizar essas linhas e espionar seus cidadãos. E não há leis contra espionar cidadãos estrangeiros. Todos os dias, centenas de milhões de mensagens vindas de todo o continente latino-americano são devoradas por órgãos de espionagem norte-americanos e armazenadas para sempre em depósitos do tamanho de cidades. Dessa forma, os fatos geográficos referentes à infraestrutura da internet têm consequências para a independência e soberania da América Latina. (ASSANGE, 2013, p. 20-21)

Neste sentido, a União das Nações Sul-Americanas (Unasul) tem se manifestado pela construção de uma rede que evite o envio de informações até servidores localizados nos EUA.

> Os ministros defenderam a construção de uma rede de comunicações sul-americana, com “pontos de troca de tráfego regional”, para “minimizar a dependência de enlaces internacionais”. Eles analisaram uma proposta de convênio entre a Unasul e o Banco Interamericano de Desenvolvimento (BID) para financiar a implantação dessa rede em cada país e recomendaram que o bloco assinasse o acordo.
> Segundo o ministro das Comunicações do Brasil, Paulo Bernardo, o projeto de interconexão vai ser importante para evitar que informações enviadas a um país vizinho tenham de cruzar o continente até chegar ao destino. “Além disso, a medida vai baratear os custos de conexão aos provedores e, consequentemente, ao consumidor. (SENADO FEDERAL, 2014, p. 29)

Em que pese abordagens de ordem técnica signifiquem um caminho importante para resolver os atuais problemas em torno da vigilância global, conforme explica Marcel Leonardi, a abordagem jurídica é fundamental para sustentar as demais formas de regulamentação.

> Como é intuitivo, o sistema jurídico tem primazia sobre as demais modalidades de regulação, pois é a única que pode definir como todas as outras devem funcionar. Ou seja, “de todas as modalidades reguladoras, a lei é a que possui a posição mais privilegiada sobre todas as outras. Isso ocorre porque a lei é a única que, por sua própria natureza, tem a capacidade de regular os demais fatores. (LEONARDI, 2011, p. 167)

A criação de uma Carta Magna Mundial da Internet é defendida por Tim Berners-Lee, criador da Web. Segundo ele, um regulamento mundial seria a solução para a garantia de direitos básicos dos usuários na rede, assim como de uma neutralidade na administração da internet (LEE, 2014).

Na perspectiva de equacionar esse cenário global de disputas em torno da neutralidade e demais princípios que devem orientar a governança da internet mundial, diversos eventos, encontros e conferências têm ocorrido com o intuito de debater questões importantes sobre a governança da internet e elaborar um documento para formalizar os pontos de consenso. Esse documento poderia ser utilizado em outros espaços de discussão e deliberação sobre governança global de internet, bem como na política interna dos países. (SANTOS, 2014)

A *Privacy International*, organização comprometida com a luta pelo direito à privacidade ao redor do mundo, estabelece alguns princípios básicos que deveriam

ser respeitados por uma legislação abrangente de proteção de dados. Dentre os princípios destaca-se a necessidade de limites para a coleta de dados, sendo que esta só poderia acontecer por meios legais e com o devido conhecimento ou consentimento do indivíduo. Além disso, as organizações responsáveis pela coleta de dados devem ser responsabilizadas pela violação de direitos. (PRIVACY INTERNATIONAL, 2015)

Em março deste ano, o governo dos EUA anunciou a intenção de abandonar seu papel central na atribuição dos nomes dos domínios na Internet em favor de um modelo de gestão global. Isso significa renunciar o controle que o Governo federal exerce sobre Corporação da Internet para Atribuição de Nomes e Números (ICANN, na sigla em inglês) – organismo encarregado de atribuir diretrizes de protocolo IP e de gerenciar o sistema de domínios. A decisão, anunciada pelo diário *The Washington Post*, é considerada uma cessão diante da pressão internacional, especialmente da União Européia, para que os Estados Unidos abandone a superintendência da estrutura do ciberespaço, que se intensificou após o escândalo de espionagem por parte das agências de inteligência norte-americanas. (TIMBERG, 2014)

Com a necessidade de desenvolvimento de diálogo entre as diversas ordens jurídicas (nacionais e supranacionais), assim como da harmonização entre os ordenamentos dos diversos Estados, é possível cogitar a existência de Estados Constitucionais cooperativos derivados do entrelaçamento das relações internacionais e supranacionais, uma vez que questões como privacidade, representam preocupação de grande parte dos Estados, estes devem agir solidariamente, em busca do bem comum. (ABREU, 2014, p. 145)

Percebe-se, recentemente, que o escândalo da espionagem estadunidense, apesar de todos os reflexos negativos, também rendeu uma consequência positiva, qual seja a atenção de vários Estados para a questão da segurança no ambiente virtual. Neste aspecto, é surpreendente que muitos países ainda não tenham regulamentação jurídica específica no que tange à proteção das relações virtuais, tal qual era a situação do Brasil até pouco tempo. Felizmente, recentemente, o Brasil tem sido exemplo ao desenvolver leis positivas para proteger e expandir os direitos dos usuários a uma web aberta, livre e universal.

Na opinião de Julian Assange, em entrevista para o jornal Folha de São Paulo, ainda levará tempo para se ter privacidade na internet. Segundo ele, no

entanto, as pessoas estão acordando para o que está acontecendo e criando demandas para algo que preserve a privacidade. (COLON, 2015)

O despertar das pessoas para a vigilância governamental e os reflexos positivos da maior preocupação mundial com o direito à privacidade servem para reforçar a idéia de que as pessoas devem continuar compartilhando conhecimentos, expondo políticos, criando ferramentas individuais para proteção de dados e pressionando os governantes à criação de leis que ofereçam mais transparência e controle em relação aos dados pessoais.

Assim, independentemente da tecnologia utilizada, é necessário o condicionado do acesso e coleta de dados pessoais a uma autorização judicial e, ainda, que os Estados violadores de normas de proteção de dados pessoais no âmbito internacional possam ser responsabilizados pelos atos que praticarem. Dessa forma, a sociedade certamente caminhará para um futuro melhor.

CONCLUSÃO

Diante da análise exposta no presente trabalho, foi possível chegar a uma solução para o problema proposto, qual seja verificar a que ponto a evolução tecnológica e os poderosos sistemas de vigilância em massa que atualmente permeiam a sociedade tendem a acarretar a diminuição da relevância social e jurídica do direito à privacidade, a ponto de ocasionar uma possível extinção desse direito.

Para tanto, foi preciso explorar o contexto social que causou a expansão da coleta de dados pessoais e o contexto jurídico que possibilitou a implementação de tais mecanismos. Perante esta conjuntura de elementos necessários ao entendimento do tema apresentado, chegou-se à conclusão de que o direito a privacidade de dados pessoais sofreu grandes limitações a partir do crescimento de políticas de combate ao terrorismo. Neste contexto, o direito tornou-se desatualizado e incapaz de conferir uma proteção satisfatória aos aspectos decorrentes da coleta e tratamentos de dados pessoais.

Frente ao caráter defasado do direito no que tange à proteção da privacidade de dados pessoais, promoveu-se uma análise acerca das modificações sofridas pela privacidade diante do desenvolvimento social e tecnológico, verificando a inconstância na definição desse direito. Além disso, através de uma reflexão acerca das consequências do mau uso de dados pessoais, pode-se estabelecer a importância desse direito, assim como o papel da proteção de dados pessoais na sua preservação. Neste sentido, foi apresentado um panorama geral da proteção de dados pessoais no ordenamento jurídico brasileiro e uma analise das principais dificuldades que estão sendo enfrentadas para elaboração de uma lei específica para a proteção de dados pessoais no Brasil.

O problema da relativização da privacidade ganha maior amplitude ao ser analisado sob o prisma do coletivo. Sendo que não apenas o indivíduo pode sofrer violação desse bem, mas toda a sociedade, o que transfere o problema para além da perspectiva meramente individual. Dessa forma, fez-se imprescindível uma análise descritiva da vigilância em massa praticada pelos governos e do alcance dos atuais programas de vigilância dos Estados Unidos com base nas revelações feitas

por Edward Snowden. Neste aspecto, foram confrontados dois interesses em conflito, de um lado a necessidade de aumento da vigilância governamental em prol da segurança pública, e de outro a necessidade de evitar que os cidadãos tenham suas privacidades violadas. Desta comparação, concluiu-se que embora os dois interesses tenham grande relevância para a sociedade, atualmente, existe um desequilíbrio recorrente entre ambos, na medida em que um direito se sobrepõe constantemente ao outro.

No estudo, verificou-se ainda que a vigilância em massa em um contexto de desequilíbrio entre os direitos favorece o surgimento de casos de abusos de poder e discriminação, especialmente quando praticada em sigilo e indiscriminadamente. Desse modo, verifica-se a necessidade mais estudos jurídicos acerca do tema, a fim de que o direito torne-se uma ferramenta capaz de conduzir a sociedade a um contexto de harmonia entre segurança pública e privacidade. Para tanto, foi proposta a utilização da ponderação entre direitos, de Alexy, com a finalidade de estabelecer um raciocínio que conduza à solução mais adequada para cada caso concreto.

Salienta-se, ainda, que a consciência pública a respeito da vigilância praticada por governos, assim como, da importância do direito à privacidade tem papel fundamental no processo de mudanças em favor da preservação desse direito. Isto se comprovou com uma série de medidas e mobilizações visando preservar a privacidade, tanto por parte dos governantes, quanto por parte de empresas de tecnologia, a partir das revelações de Snowden e da reação negativa da opinião pública diante dos “escândalos da vigilância”.

Por meio de uma reflexão sobre os possíveis cenários da vigilância no futuro, foi destacada a necessidade de que as tecnologias além de possibilitar uma vigilância do governo sobre os cidadãos, efetivando assim a segurança pública, devem também possibilitar uma vigilância dos cidadãos sobre os governos, ou seja, uma maior transparência e responsabilização dos governos acerca da coleta e tratamento de dados pessoais. Neste sentido, constatou-se que o Direito Internacional Público tem o papel fundamental de possibilitar a responsabilização dos Estados por possíveis violações decorrentes da vigilância em massa.

Cabe ressaltar ainda, que em se tratando de obter transparência pública os meios legais esbarram em seus próprios limites, pois os sistemas de vigilância são em grande parte desenvolvidos em sigilo e tendem a atuar da mesma maneira, dificultando assim uma regulação unicamente por meio de leis.

Ademais, o aumento dos debates mundiais sobre o tema, aliado ao surgimento de diversas propostas, tanto de ordem técnica, quanto de ordem jurídica, visando solucionar o problema da perda de privacidade dá sinais de que as formas de controle democráticas que podem preservar este direito ainda não estão totalmente exauridas e que a capacidade inventiva do ser humano será capaz de resolver também este problema.

Conclui-se, portanto, que embora o direito à privacidade esteja constantemente em risco diante dos poderosos sistemas de vigilância em massa, falar em extinção desse direito na atual sociedade, ainda possui certa conotação alarmista que subestima a capacidade humana de adaptação às novas situações e também a própria capacidade de evolução e renovação do Direito como instrumento regulador de novas situações jurídicas. No entanto, há de se ter consciência de que permanecem latentes os perigos associados ao mau uso das tecnologias de vigilância em massa e, portanto, a exposição de políticos, a divulgação ou compartilhamento de conhecimentos e a pressão da opinião pública são fundamentais para estimular a criação de instrumentos capazes de limitar e regular o poder de vigilância na atual sociedade.

REFERÊNCIAS

ABREU, M. B. G. **A proteção à vida privada, intimidade e sigilo de dados na constituição brasileira de 1988 e a espionagem internacional**. 2014. 190 f. Dissertação (mestrado em Direito Público) – Programa de Pós-Graduação em Direito (PPGD) da Universidade Federal da Bahia, Salvador, 2014. Disponível em: <https://repositorio.ufba.br/ri/handle/ri/16597>. Acesso em: 01 nov. 2015.

ALEXY, R. **Teoria dos Direitos Fundamentais**; tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ANISTIA INTERNACIONAL. 7 maneiras que o mundo mudou graças a Edward Snowden. 12 jun. 2015. Disponível em: <https://anistia.org.br/noticias/7-maneiras-que-o-mundo-mudou-gracas-edward-snowden/>. Acesso em: 17 out. 2015.

ASSANGE, J. et al. **Cypherpunks**: liberdade e o futuro da internet; tradução de Cristina Yamagami. São Paulo: Boitempo, 2013.

BAUMAN, Z. **Vigilância líquida**: diálogos com David Lyon/Zygmunt Bauman; tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BERG, J. L. Nsa e o monitoramento dos Eua, parte 6: como isso me afeta? In: Jornal GGN, 2013. Disponível em: <http://jornalggn.com.br/blog/jluizberg/nsa-e-o-monitoramento-dos-eua-parte-6-como-isso-me-afeta>. Acesso em: 30 set. 2015.

BIONI, B. R.; RIBEIRO, M. M. A Transposição da Dicotomia entre o Público e o Privado. **JOTA**. [Publicado em 25 set. 2015]. 2015. Disponível em: <http://jota.info/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado>. Acesso em: 30 set. 2015.

BOYD, d.; CRAWFORD, K. Six Provocations for Big Data. In: A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431>. Acesso em: 23 set. 2015.

BRASIL. Lei n. 12.414, de 9 de junho de 2011. Lei do Cadastro Positivo. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 10 jun. 2011. 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 28 set. 2015.

_____. Lei n. 12.527 de 18 de novembro de 2011. Lei de Acesso à Informação. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. 2011b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 28 set. 2015.

_____. Lei n. 12.965 de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 set. 2015.

_____. Ministério da Justiça. Anteprojeto de Lei para a Proteção de Dados Pessoais. [Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural]. Brasília, 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 30 set. 2015.

_____. Ministério das Relações Exteriores. Brasil e Alemanha apresentam à ONU projeto de resolução sobre o direito à privacidade na era digital. [Nota de imprensa: n.º 376 publicada em 01 de novembro de 2013]. 2013. Disponível em: <http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=3424:brasil-e-alemanha-apresentam-a-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital&catid=42&lang=pt-BR&Itemid=280>. Acesso em: 13 nov. 2015.

BRUNO, F. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **FAMECOS**, v. 1, n. 36, p. 10-16, 2008. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410/3309>. Acesso em: 22 jun. 2015.

CABRAL, A. M. R. SOCIEDADE PÓS-MODERNA: O PODER DA INFORMAÇÃO – O PODER DE INFORMAR. Escola de Biblioteconomia UFMG, v. 21, n. 2, p. 2013-223, 1992. Disponível em: <http://www.brapci.ufpr.br/documento.php?dd0=0000002495&dd1=3e300>. Acesso em: 15 out. 2015.

CARLONI, G. L. B. S. C. **Privacidade e Inovação na Era do *Big Data***. 2013. 49 f. Artigo Científico (Graduação em Direito) - Fundação Getulio Vargas, Rio de Janeiro, 2013. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/12664>. Acesso em: 25 set. 2015.

CARTILHA DE SEGURANÇA PARA INTERNET, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em:

<http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 02 nov. 2015.

CASTRO, C. S. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. 2003. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf>. Acesso em: 01 nov. 2015.

CASTRO, R. B. **Redes e Vigilância**: Uma experiência de cartografia psicossocial. 2008. 177 f. Dissertação (Mestrado em Psicossociologia de Comunidades e Ecologia Social) – UFRJ / IP / Programa de Pós-graduação em Psicossociologia de Comunidades e Ecologia Social, 2008.

CERVONE, F. Tratado internacional é a melhor arma contra espionagem dos EUA, diz especialista americano. In: R7 Notícias. Nova York, 2013. Disponível em: <http://noticias.r7.com/internacional/tratado-internacional-e-a-melhor-arma-contra-espionagem-dos-eua-diz-especialista-americano-24092013>. Acesso em: 02 out. 2015.

COLON, L. 'Ainda levará tempo para se ter privacidade na internet', diz Assange. In: Folha de São Paulo. 2015. Disponível em: <http://www1.folha.uol.com.br/mundo/2015/02/1587247-ainda-levara-tempo-para-se-ter-privacidade-na-internet-diz-assange.shtml>. Acesso em: 06 nov. 2015.

DONEDA, D. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/viewArticle/1315>. Acesso em: 15 out. 2015.

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

ESTADOS UNIDOS. Public Law 107–56. 2001. PATRIOT ACT. Disponível em: <http://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf>. Acesso em: 29 set. 2015.

FACEBOOK. **Cookies, pixels e tecnologias semelhantes**. 2015c. [Política de Uso de Cookies]. Disponível em: < https://pt-br.facebook.com/help/cookies>. Acesso em: 29 set. 2015.

_____. **Declaração de Direitos e Responsabilidades**. 2015a. [Termos de Serviços]. Disponível em: <https://pt-br.facebook.com/legal/terms>. Acesso em: 29 set. 2015.

_____. **Política de Dados**. 2015b. [Política de Privacidade]. Disponível em: <https://pt-br.facebook.com/about/privacy>. Acesso em: 29 set. 2015.

FUCHS, C. Como podemos definir vigilância? **MATRIZes**, v. 5, n. 1, p. 109-136, 2011. Disponível em: <http://www.matrizes.usp.br/index.php/matrizes/article/view/203/pdf>. Acesso em: 10 out. 2015.

FOUCAULT, M. **Vigiar e Punir**: nascimento da prisão; tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

GIDDENS, A. **The constitution of society**: Outline of the theory of structuration. Cambridge: Polity Press. 1984.

GOOGLE. **Política de Privacidade**. 2005. [Versão arquivada de 14 de outubro de 2005]. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/archive/20051014/>. Acesso em: 20 ago. 2015.

GOOGLE. **Política de Privacidade**. 2015. [Versão atual de 19 de agosto de 2015]. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/>. Acesso em: 20 ago. 2015.

GOULART, G. D. 7. CONDICIONAMENTO, LIBERDADE E PRIVACIDADE: COMPREENDENDO AS NOVAS TECNOLOGIAS POR MEIO DO “ADMIRÁVEL MUNDO NOVO". **DIALOGOS DO DIREITO**, v. 4, n. 6, p. 87-109, 2014. Disponível em: <http://ojs.cesuca.edu.br/index.php/dialogosdodireito/article/view/580/403>. Acesso em: 22 jun. 2015.

_____. O Impacto das Novas Tecnologias nos Direitos Humanos e Fundamentais: O Acesso à Internet e a Liberdade de Expressão. **Revista Direitos Emergentes na Sociedade Global**, v. 1, n. 4, p. 145-168, 2012. Disponível em:<http://cascavel.ufsm.br/revistas/ojs-2.2.2/index.php/REDESG/article/view/5955#.VkpEgNKrQsZ>. Acesso em: 27 out. 2015.

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

HUFFINGTON POST. Tech. Facebook's Zuckerberg Says Privacy No Longer A 'Social Norm' (VIDEO). 18 mar. 2010. Disponível em: <http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html?>. Acesso em: 15 set. 2015.

LEE, T. B. Uma Carta Magna para a Internet. In: TED2014. [Palestra gravada em março de 2014]. 2014. Disponível em: <https://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web?language=pt-br>. Acesso em: 15 out. 2015.

LEONARDI, M. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011.

LYON, D. **Surveillance studies**: an overview. Cambridge UK: Polity Press, 2007.

MACHADO, J. M. S. **CAMINHOS PARA A TUTELA DA PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO**: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil. 2014. 186 f. Tese (Doutorado em Direito Constitucional) – Universidade de Fortaleza, Fortaleza, 2014. Disponível em: <http://uol01.unifor.br/oul/conteudosite/F86027120141111150021922278/Tese.pdf>. Acesso em: 25 set. 2015.

MARQUES, R. M.; PINHEIRO, M. M. Informação e poder na arena da Internet. **Informação & Sociedade: Estudos**, v. 24, n. 1, p. 47-60, 2014. Disponível em: <http://www.okara.ufpb.br/ojs/index.php/ies/article/view/15252>. Acesso em: 15 out. 2015.

MARTINS, A. Censura política no Facebook? In: Blog da Redação, [Publicado em 18 set. 2015]. Disponível em: <http://outraspalavras.net/blog/2015/09/18/censura-politica-no-facebook/>. Acesso em: 25 set. 2015.

MIRANDA, Y. P.; SOUSA, R. F. Sistemas de Internet e a Proteção da Privacidade do Usuário: uma análise a partir dos termos de uso. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, v. 10, n. 1, p. 029-038, 2015. Disponível em: <http://www.biblionline.ufpb.br/ojs2/index.php/pbcib/article/view/22965>. Acesso em: 16 ago. 2015.

O GLOBO. Gigantes da tecnologia exigem reforma na política de vigilância dos EUA. In: Tecnologia. 26 mar. 2015. Disponível em:

<http://oglobo.globo.com/sociedade/tecnologia/gigantes-da-tecnologia-exigem-reforma-na-politica-de-vigilancia-dos-eua-15703383>. Acesso em: 17 out. 2015.

PAESANI, L. M. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 5. ed. São Paulo: Atlas, 2012.

PAGLIUSI, P. Brasil na mira dos 'Five Eyes'. In: Convergência Digital, 2014. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36338&sid=127#.VibISNKrTMw>. Acesso em: 28 set. 2015.

PIOVESAN, F. **Direitos Humanos e o Direito Constitucional Internacional**. In: Caderno de Direito Constitucional, Porto Alegre, Módulo V, 2006.

PRIVACY INTERNATIONAL. What is Privacy. London, [2015?]. Disponível em: <https://www.privacyinternational.org/node/54>. Acesso em: 28 set. 2015.

RAMOS, P. R. B.; COSTA, O. J. G. RESPONSABILIDADE INTERNACIONAL DO ESTADO E SOCIEDADE INTERNACIONAL: A CONSOLIDAÇÃO DA COMUNIDADE INTERNACIONAL DE ESTADOS E A SUA INFLUENCIA NO PROJETO DE ARTIGOS SOBRE RESPONSABILIDADE DO ESTADO POR ATOS INTERNACIONALMENTE ILÍCITOS. [2012?]. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=31b91e3a8737fd8d>. Acesso em: 10 nov. 2015.

REGALADO, A. Espionagem é ruim para os negócios. In: MIT Technology Review. 21 mar. 2014. Disponível em: <http://www.technologyreview.com.br/printer_friendly_article.aspx?id=44995>. Acesso em: 17 out. 2015.

RICHTER, W. LEAKED: German Government Warns Key Entities Not To Use Windows 8 – Links The NSA. In: Wolf Street, 2013. Disponível em: <http://wolfstreet.com/2013/08/22/leaked-german-government-warns-key-entities-not-to-use-windows-8-links-the-nsa/>. Acesso em: 26 set. 2015.

RODOTÀ, S. **A vida na Sociedade da Vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANDEL, M. J. **Justiça**: O que é fazer a coisa certa; tradução de Heloísa Matias e Maria Alice Máximo. 6 ed. Rio de Janeiro: Civilização Brasileira, 2012.

SANTOS, V. W. O. Governança da internet no Brasil e no mundo: a disputa em torno do conceito de neutralidade da rede. In: Laboratório de Estudos Avançados em Jornalismo da Unicamp. 2014. Disponível em: <http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542014000400009&lng=pt&nrm=isso>. Acesso em: 01 nov. 2015.

SENADO FEDERAL. **EM DISCUSSÃO!**: Os principais debates do Senado Federal, Brasília, Ano 5, n. 21, 2014. Disponível em: <http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/espionagem.pdf>. Acesso em: 30 set. 2015.

SILVA, H. L. Monitorização da internet: onde fica o direito à privacidade? **Verbo Jurídico**, 2006. Disponível em: <http://www.verbojuridico.net/doutrina/tecnologia/monitorizacaointernet.pdf>. Acesso em: 16 ago. 2015.

SIQUEIRA, E. Incrível: maioria apóia o fim da privacidade. [MUNDO VIRTUAL]. **O Estado de São Paulo**, São Paulo, 29 ago. 2006. Disponível em: <http://observatoriodaimprensa.com.br/jornal-de-debates/o_estado_de_s_paulo__31052/>. Acesso em: 26 set. 2015.

SNOWDEN, E. Snowden: nós mudamos a forma como o mundo percebe a vigilância em massa. In: ANISTIA INTERNACIONAL BRASIL. 07 jun. 2015. Disponível em: <https://anistia.org.br/snowden-nos-mudamos-forma-como-o-mundo-percebe-vigilancia-em-massa/>. Acesso em: 15 out. 2015.

TAURION, C. O estágio atual do Big Data no Brasil. [Entrevista disponibilizada em 3 de junho de 2013, a Revista Powerchannel]. 2013. Disponível em: <http://www.powerchannel.com.br/2013/06/03/cezar-taurion-o-estagio-atual-do-big-data-no-brasil/>. Acesso em: 29 set. 2015.

TEDGLOBAL. **Glenn Greenwald**: Por que a privacidade é importante. [Palestra realizada em outubro de 2014]. 2014. Disponível em: <http://www.ted.com/talks/glenn_greenwald_why_privacy_matters?language=pt-br>. Acesso em: 26 set. 2015.

TIMBERG. C. U.S. to relinquish remaining control over the Internet. In: The Washington Post. 2014. Disponível em: <https://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html>. Acesso em: 01 nov. 2015.

UCHOA, P. Obama promete rever espionagem, mas diz que mundo hoje é mais estável. **BBC Brasil**, Nova York, 24 set. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/09/130924_obama_espionagem_ru>. Acesso em: 10 out. 2015.

UNESCO. DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS [Proclamada em 10 de dezembro de 1948]. Brasília, 1998. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 02 nov. 2015.

VAIDHYANATHAN, S. **A Googlelização de Tudo**: (e por que devemos nos preocupar): a ameaça do controle total da informação por meio da maior e mais bem-sucedida empresa do mundo virtual; tradução de Jeferson Luiz Camargo. São Paulo: Cultrix, 2011.

VIANNA, T. L. **Transparência pública, opacidade privada**: o Direito como instrumento de limitação do poder na sociedade de controle. 2006. 206 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade Federal do Paraná, Curitiba, 2006.

WAYBACK MACHINE. Política de Privacidade do Google no ano 2000. [Documento consultado no site Internet Archive Wayback Machine]. Disponível em: <https://archive.org/web/>. Acesso em: 20 ago. 2015.