ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

# Da expansão das redes sociais à ruína do direito à privacidade: uma análise jurídica sobre o *Big Data* e seus efeitos

Caroline Sampaio Benini Souza[1]
Lívia França de Oliveira e Silva[2]
Mariana de Sales Tomaz[3]
Mylena Braga Ramires [4]
Pietra de Paula Alvim [5]

## RESUMO

O presente artigo teve por objetivo geral analisar como a expansão da tecnologia através das redes sociais e de ferramentas de armazenamento de dados impactou a vida privada através da problemática coleta de informações pessoais, tão expandida no século XXI. A metodologia utilizada foi pesquisa bibliográfica e documental. A partir do estudo pode evidenciar como o direito à privacidade é comprometido quando violado por esses meios que, por sua vez, vendem informações particulares de seus usuários para empresas que criam padrões, a partir dos dados coletados, com o intuito de revelar tendências a serem empregadas em estratégias digitais, gerando, assim, mais consumo e influenciando em decisões importantes, como sociais e políticas. A discussão proposta apresenta exemplos pertinentes para a observância do fenômeno

[1] Graduanda do curso de Direito das Faculdades Integradas Vianna Júnior
[2] Graduanda do curso de Direito das Faculdades Integradas Vianna Júnior
[3] Graduanda do curso de Direito das Faculdades Integradas Vianna Júnior
[4] Graduanda do curso de Direito das Faculdades Integradas Vianna Júnior
[5] Graduanda do curso de Direito das Faculdades Integradas Vianna Júnior

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

em questão, como, por exemplo, o caso *Cambridge Analytica* e o programa *Deep Packet Inspection*, por meio de um estudo sobre o *Big Data*.

## INTRODUÇÃO

A internet tem alterado, constantemente, as transformações da convivência humana, sendo inserida na vida de milhões de pessoas no mundo e, com isso, facilitando a comunicação entre os usuários, por meio do acesso e compartilhamento de dados e informações. Todavia, essa facilidade traz consigo alguns perigos à segurança do usuário, implicando diretamente no seu direito à privacidade. Desse modo, será verificado como tal problemática acontece, as motivações e como nosso ordenamento jurídico e as jurisprudências se posicionam no que se refere a este tema.

Para o alcance dos objetivos definidos acima, o presente artigo trata de estudos e análises sobre os ambientes virtuais e uso das redes sociais, sob a ótica da relação entre o Big Data e o direito à privacidade, garantido na Constituição Federal, verificando-se as falhas cometidas pelas empresas e pelos usuários e como a legislação brasileira age em casos assim, mostrando que só a existência do direito à privacidade não garante sua aplicabilidade.

A respeito dos Direitos Fundamentais, o debate se realiza através do direito à privacidade e a reflexão sobre a garantia de tal direito no universo das redes sociais, junto à análise do atual contexto histórico das redes e do comportamento dos usuários.

A pesquisa, ao pautar-se no uso das redes sociais e de sites em geral, tendo por base o sistema Big Data e a interligação com a garantia à privacidade, desenvolve-se em três capítulos. Inicia-se com uma abordagem jurídica que retrata como o direito à privacidade se encaixa e permanece vigente na sociedade da informação; logo após, são demonstrados os motivos, como acontece a coleta de dados e em que medida interferem na violação da referida garantia, utilizando-se casos reais para comprovar tal

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

fato. Por fim, são apresentadas as principais considerações feitas após o estudo abordado.

## 1 O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

O direito à privacidade remete, no campo jurídico, ao "*right to privacy*". A privacidade pode ser definida, assim, como o direito de estar só ou, talvez mais preciso, o direito de ser deixado só ("*right to be let alone*"). Tais termos foram abordados no grande marco doutrinário criado por Samuel Dennis Warren e Louis Demitz Brandeis em 1890, nos Estados Unidos (EUA), no artigo intitulado *Right to privacy*, o qual foi publicado na *Harward Law Review* (NOJIRI, 2005).

Demitz e Brandeis, ao analisarem os precedentes judiciais da Suprema Corte dos EUA, concluíram que deveria haver uma proteção pelas Cortes ao denominado *right to privacy*, sendo este o direito de o indivíduo estar só com seus pensamentos, emoções e sentimentos, independente da forma de expressão, seja ela por manifestos em cartas, diálogos, livros, entre outros. Portanto, refere-se a não interferência pelo Estado na vida do indivíduo. Todavia, deve-se entender a privacidade não apenas como a não interferência do Estado na vida privada das pessoas, mas, também, como o poder de se reivindicar a este órgão a tutela dessa privacidade, protegendo o indivíduo de terceiros (VIEIRA, 2007).

Após isso, houve um grande avanço doutrinário e jurisprudencial sobre a temática e o direito à privacidade tomou contornos internacionais, principalmente ao ser reconhecido pela Declaração Universal dos Direitos do homem (1948), conforme dispõe o artigo XII:

> Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

> honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

No Brasil, a Constituição Federal de 1988, o mais alto diploma normativo da República Federativa do Brasil, o qual orienta os demais e prevalece sobre eles, aborda, em seu art. 5º, os direitos fundamentais. Entre eles, está o direito à liberdade, à igualdade, à propriedade e à privacidade, estudada por nós neste artigo.

Afirma, portanto:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988)

Além disso, apesar de o direito à privacidade ter tomado proporções maiores e atingido nível constitucional, cabe ressaltar que é necessário que haja sempre uma atualização do direito para englobar as mudanças que ocorrem na sociedade. Como dito pelo artigo "*right to privacy"* (apud NOJIRI, 2005), anteriormente citado:

> Que o indivíduo deva receber plena proteção de sua pessoa e de sua propriedade é um princípio antigo como o common law. Não obstante, tem sido necessário, de tempos em tempos, redefinir a natureza exata e a extensão dessa proteção. As transformações políticas, sociais e econômicas exigem o reconhecimento de novos direitos e o common law, com sua eterna juventude, cresce para satisfazer as demandas da sociedade

Logo, mesmo em 1890, os estudiosos já visualizavam a necessidade de o Direito acompanhar as transformações sociais.

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

Nesse sentido, sabe-se que os meios de comunicação e as tecnologias, além de estarem presentes na vida de todos os indivíduos, são dotados de novos avanços diariamente, avanços estes que a maioria das pessoas não tem ciência sobre a repercussão em sua vida pessoal e privada. Dessa maneira, tais tecnologias, muitas vezes através das redes sociais tão usadas atualmente, envolvem a violação de privacidade e a publicação deliberada de dados pessoais presentes nesses meios.

Assim, segundo Boff e Fortes (2014), a atual geração tecnológica tem como grande elemento catalizador das empresas de tecnologia da informação e comunicação a violação e a comercialização de dados pessoais.

A partir deste desafio contemporâneo – cenário social, político e econômico em que a principal riqueza é a informação – destaca-se o abusivo uso da tecnologia e das redes sociais para fiscalização dos indivíduos e obtenção de dados, permanecendo sempre vigiados.

Pode-se, então, comparar tal fenômeno ao sistema desenvolvido pelo filósofo e jurista inglês Jeremy Bentham denominado panoptismo (século XVIII), em que se criou um projeto de prisão circular, na qual o observador estabelecido no centro poderia enxergar todas as celas em que estivessem os presos, sem que estes pudessem ver o observador. Ou seja, os presos nunca sabiam se estavam sendo realmente observados ou não, dúvida esta que incentivaria a boa conduta. Posteriormente, Michel Foucault retomou o conceito criado por Bentham e destacou a importância do panóptico como ferramenta de poder ao afirmar: “quanto maior o número de informações em relação aos indivíduos, maior a possibilidade de controle de comportamento desses indivíduos” (ANDRÉA, 2019).

Logo, para o referido autor, o que se vê é que a obtenção de dados pessoais e sigilosos dos indivíduos, através da obstrução do direito à privacidade por meio, principalmente, de *smartphones*, atrelado à majoritária adesão de pessoas às redes sociais (*facebook, instagram, twitter*) nas últimas décadas, concretiza o surgimento de um verdadeiro panóptico digital em pleno século XXI. E, além disso, não se tem como

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

saber quem são os reais observadores e o que estão fazendo com os dados coletados. Tal realidade torna, assim, muito atual as visões de Foucault e Bentham.

Diante dessa violação, recentes casos e ferramentas, os quais serão tratados subsequentemente, mostram que esse fato está presente não só no Brasil – onde, inclusive, o legislador buscou amenizar tais ocorrências criando lei ordinária que trata sobre a temática – como nos diversos países do globo, trazendo consequências ao cumprimento efetivo da garantia à privacidade, prevista na Constituição Federal e gerando efeitos na vida pessoal dos indivíduos, abordados *a posteriori.*

## 2 CASOS EM QUE HÁ QUEBRA DO DIREITO À PRIVACIDADE

Neste tópico, serão ilustrados assuntos que apresentam a abordagem em questão aplicada no desdobramento de casos e ferramentas que foram estudadas para a produção do presente artigo. Assim, será tratado, primeiramente, sobre a base da problemática, compelida na forma do sistema do *Big Data* e sua repercussão no setor privado dos indivíduos. Desdobra-se tal programa no emblemático caso do *Cambridge Analytica* e, ao final, ao sistema da *Deep Packet Inspection*, recém implantado no Brasil.

### 2.1 Fenômeno do *Big Data*

Por meio das facilidades tecnológicas existentes no atual cenário social e profissional e nos campos da gestão e da pesquisa, a capacidade de captação de dados foi elevada a instâncias inimagináveis, chegando aos conjuntos de dados massivos.

De acordo com Dumbill (*apud* LOTT; CIANCONI, 2012), em 1997, na NASA, o termo *big data* surgiu para definir, embora não formando um conceito objetivo, a

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

condição de uma base de dados que, pelo volume, velocidade e variedade de dados, excede as capacidades técnicas e de infraestrutura para seu armazenamento, processamento e visualização. Ao contrário dos tempos em que o registro das informações era feito basicamente em meio físico, hoje, a ampla presença de dispositivos óticos e sensores dos mais diversos tipos permite a conversão de objetos, fatos e eventos, do real para o digital, praticamente no momento em que eles ocorrem, o que avança a esfera tecnológica e atinge setores da vida privada.

Tal descrição sobre este termo, que está em alta, foi abordada no artigo "Privacidade em *Big Data*: panorama e agenda de pesquisa", feito por Celina Silva e Elaine Rodrigues (2017), que ressaltam que:

> Em um mercado altamente competitivo ou em contextos administrativos de alta complexidade, encontrar novas maneiras de interpretar os dados e processá-los de maneira mais rápida tem se mostrado uma capacidade de diferenciação perante as empresas. A variedade está relacionada à capacidade de analisar uma extensa gama de tipos de dados e fontes, incluindo dados estruturados, semi-estruturados e não estruturados que, como Big Data, toma a forma de mensagens, imagens e outros tipos de dados em redes sociais, sensores, GPS de celulares, dentre outros.

De acordo com Natanael Galdino (2019), em seu trabalho intitulado "*Big Data*: Ferramentas e Aplicabilidade", os dados que são analisados pelo sistema *Big Dataem análise* são retirados dos mais variados sites e redes sociais que possuem um acesso deliberado e, muitas vezes, não permitido pelos usuários; além de compras pelo cartão de crédito, biometria e outros meios de comunicação, em que há a troca de dados pessoais.

É comum nesse sistema a utilização dos termos 3Vs, cujo objetivo é manter as plataformas e os sistemas em harmonia, que são: o "volume", que se refere a quantidade dos dados acumulados; a "variedade", que é uma taxa de transmissão dos dados; a "velocidade", que se refere à taxa de transmissão de dados. Entretanto, foram

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

agregados mais 2Vs ao *Big Data*: “veracidade”, para verificar se os dados são confiáveis ou não, e o “valor”, que é o resultado final no uso das ferramentas de *Big Data*. (SILVA; RODRIGUES, 2017)

Entretanto, a incerteza em relação ao sistema em questão é quanto ao fornecimento de dados pessoais e o direito à privacidade dos indivíduos. A tendência é de crescimento dos problemas de privacidade, por conta da produção de dados e a exposição de informações de teor privado, coletadas sem plena consciência dos indivíduos. Nesse sentido, Boydet Crawford (*apud* SILVA; RODRIGUES, 2017) coloca questões como: Quais dados são coletados e quais não? Qual o motivo disso? O que é usado e o que não é? Quais são os desdobramentos dessa seleção? Quais fatores fundamentais ou críticos devem ser considerados para pleno entendimento de um fenômeno particular ou condição? Essas questões apontam para a necessidade de uma abordagem crítica sobre *Big Data* em termos do entendimento sobre a sua essência, uso e efeitos e abordagem no âmbito privado.

O que se percebe, a partir do exposto da relação entre *Big Data*, acesso de dados e direito à privacidade, e que será mostrado mais adiante, é uma tendência forte de comprometimento e, conseqüente, quebra da garantia à vida privada em questão, mediante sistemas de dispositivos digitais, os quais transmitem informações diversas, algumas transparentes para o usuário, outras carregadas e compartilhadas por ele enquanto ator no próprio sistema. Mas, conforme as autoras Celina Silva e Elaine Rodrigues (2017), em algum momento do processo de aquisição de dados, há sempre intervenção humana para definir o que é transmitido ou qual uso será dado para essas informações; e, seja aceitando termos e condições contratuais, seja deixando um dispositivo exposto ou vulnerável, os efeitos dessa prática recaem sobre o indivíduo.

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

## 2.2 *Deep Packet Inspection*

Diante da análise feita anteriormente, é preciso promover o estudo crítico em torno do tema e sua relação com os direitos fundamentais no ciberespaço, em especial, o direito à privacidade, no presente item, sob o foco do *Deep Packet Inspection* (DPI), desdobramento do sistema *Big Data*.

Nesse contexto, a tecnologia do DPI, provinda em decorrência do sistema do *Big Data*, é capaz de rastrear e registrar todos os movimentos de seus usuários, revelando informações detalhadas sobre o seu estilo de vida e suas escolhas pessoais, além de coletarem dados confidenciais, como localização e mensagem de texto, por exemplo, gerenciando o tráfego na rede. Assim, esse recurso possibilita que operadoras de rede realizem uma inspeção profunda - o que dá origem à denominação - dos pacotes de dados que transitam na infraestrutura de rede dessas operadoras, objetivando uma otimização dos custos, a partir do conhecimento do tráfego demandado pelos usuários. (FORTES; MIGLIAVACCA, 2019).

A título ilustrativo, a imagem abaixo retrata como a inspeção profunda de dados, por meio da DPI em questão, atua para conseguir os dados privados dos indivíduos:

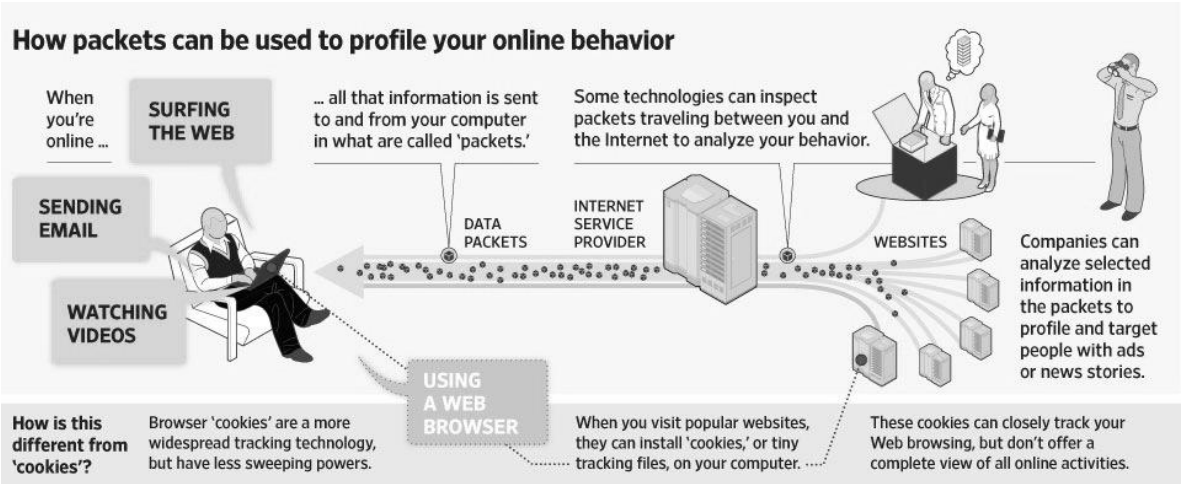


Figura 1 – *Deep Packet Inspection (DPI)*
Fonte: STECKLOW; SONNE, 2010 (apud FORTES; MIGLIAVACCA, 2019)

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

Desse modo, como explica o advogado e colunista no site Jus, Cláudio Ralves (2019), nos dias atuais, a abundante inovação tecnológica, através dessas ferramentas de captura de informações privadas, e o efeito rede mudaram a perspectiva de privacidade, sob o enfoque dos bancos de dados compartilhados via internet e o grande volume de informações processadas mecanicamente e de forma instantânea, fez com que os setores da sociedade enxergassem o direito da privacidade com um novo prisma. Afinal, esse tipo de plataforma traz riscos a todos, uma vez que possibilita a dissipação de dados pessoais e facilita a prática de atividades ilícitas por parte de qualquer pessoa mal-intencionadas, estando todos sujeitos a esses riscos.

> E como se não bastassem os acontecimentos envolvendo a violação de privacidade e a publicação deliberada desses dados, a atual geração tecnológica tem como grande elemento catalizador das empresas de tecnologia da informação e comunicação a violação e a comercialização de dados pessoais. (FORTES, MIGLIAVACCA, 2019).

Um exemplo dessa questão é a multinacional britânica *Phorm*, recém-chegada ao Brasil, que explora os dados dos usuários no ciberespaço e tem como objetivo auxiliar os provedores de Internet no uso do recurso mencionado chamado Inspeção Profunda de Pacotes de Rede (DPI – *Deep Packet Inspection*), e utilizam desses dados para a construção de perfis quase plenos de todos os usuários da *Web,* para a utilização futura na padronização de serviços de publicidade, sendo isso, uma concretização da comercialização de dados pessoais, anteriormente citada para expansão de vendas de produtos.

Conforme afirma Marília Monteiro (apud FORTES; MIGLIAVACCA, 2019), a DPI é um recurso tecnológico cujos benefícios são altamente questionáveis por permitir que provedores de acesso à Internet obtenham os dados pessoais dos usuários e monitorem a utilização da rede por esses usuários, sendo uma clara violação de

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

privacidade. Para a pesquisadora, a identificação do tráfego dos usuários poderia provocar:

> […] ações desejadas pelo poder público, como controle de conteúdos acessados por cidadãos (censura), ou orientar interesses empresariais, como diferenciação de tráfego para serviços pouco desejados e competitivos aos seus serviços", o que já ocorre em países com regimes governamentais democráticos e não democráticos. [...] ( MONTEIRO, apud FORTES; MIGLIAVACCA, 2019)

Nesse sentido, segundo a resolução CGI.br/RES/2012/008/P (2012), o recurso tecnológico da DPI fere alguns dos princípios para a governança e uso da *Internet* no Brasil, quais sejam o da neutralidade da rede, a partir da filtragem e geração de tráfego de acordo com motivos políticos, comerciais, religiosos, culturais e econômicos, e o da padronização da operação da *Internet* no país. Ademais, ao manifestar uma postura de não recomendação de uso pelos provedores de acesso à rede no Brasil, a CGI.br tornou claro que o uso do DPI traz graves ameaças à privacidade dos usuários. (FORTES; MIGLIAVACCA, 2019).

Diante do exposto, pode-se concluir que nenhuma rede social está isenta de captação de dados por sistemas de tecnologia justamente criados com esse fim. Portanto, os usuários estão, a todo momento, sujeitos a serem observados por pessoas desconhecidas que ingressam nas redes e obtêm informações pessoais dos cidadãos, podendo estas informações ser compartilhadas e vendidas, comprometendo o direito fundamental da privacidade previsto na Constituição Federal. Por fim, é possível destacar que há uma problemática jurídica em questão, decorrente do acesso ilimitado a dados no ciberespaço e o modo como o Poder Judiciário e Legislativo se comportam frente a tais casos.

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

## 2.3 Caso *Cambridge Analytica e Facebook*

A expansão da tecnologia no século XXI começou com o sonho de um mundo conectado, um espaço para se dividir experiências, em que as pessoas poderiam se sentir menos sozinhas. Porém, esse sonho se transformou e o mundo conectado converteu essas pessoas em mercadoria para empresas que coletam dados nas diversas redes sociais existentes atualmente.

Em decorrência do *Deep Packet Inspection* e, consequentemente, do *Big Data*, analisados anteriormente, o professor David Carrol explica, no documentário "Privacidade Hackeada" (2019), que toda atividade online é conectada em tempo real à identidade virtual, dando a qualquer comprador acesso direto ao seu impulso emocional.

Nessa perspectiva, segundo o jornal britânico *The Guardian* (apud ROSA, 2018), a empresa de assessoria política *Cambridge Analytica* usou informações privadas de mais de 50 milhões de usuários do *Facebook*, sendo 400 mil brasileiros, para a criação de campanhas políticas manipuladas, trabalhando, por exemplo, para a de Donald Trump e para o fenômeno do Brexit (saída do Reino Unido da União Europeia), sendo um esquema de coleta, venda e uso indevido de dados de milhões de americanos.

Segundo Murico Roncolato (2018), a empresa em questão montou "psicográficos", que consistem em uma espécie de perfis baseados em traços da personalidade, a fim de formar opiniões e direcionar votos ao candidato republicano – prática conhecida no marketing político como "microtargeting".

A *Cambridge Analytica* conseguiu colher esses dados privados através de um teste de personalidade no *Facebook*, o qual atuava quando o usuário realizava um *quiz*, possibilitando ter acesso a todas as suas informações e de seus amigos, incluindo conversas privadas, as quais eram armazenadas para, depois, serem vendidas sem o conhecimento e consentimento deles, fatos que posteriormente foram confirmados pelo *Facebook*. Esse fato permitiu que, por meio do rastreamento do que os usuários mais

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

visualizavam nas redes, a empresa soubesse as principais inclinações políticas e sociais dos indivíduos.

Conforme Diogo Queiroz de Andrade (2018), o objetivo da coleta de dados, em meio às eleições dos EUA, em 2016, era usar as redes sociais para manipular emoções, enfatizar uma campanha política através do medo e da esperança, bombardeando os usuários com notícias manipuladas. O autor ainda pondera sobre a filmagem gravada por Britanny Kaiser, ex-funcionária da *Cambridge Analytica*, e publicada pelo veículo de informação *Open Democracym*, em que Alexander Nix, ex-diretor de operações da empresa, discute como impactou nas eleições de Trindad e Tobago, em 2007, além dos EUA, em 2016.

Logo, após as conversas vazadas de Alexander Nix repercutirem no mundo todo, a empresa *Cambridge Analytica* decretou falência. Além disso, a Comissão Federal de Comércio dos Estados Unidos multou o *Facebook* em 5 bilhões de dólares, por violar o direito à privacidade dos usuários.

Em suma, pode-se destacar que o caso *Cambridge Analytica* gerou impactos radicais no mundo inteiro, alertando sobre a vulnerabilidade dessas redes virtuais. Dessa maneira, tanto a Europa quanto o Brasil criaram leis de proteção de dados, posicionando-se contra o tratamento indevido de dados pessoais por empresas e consolidando-se favoráveis à segurança da garantia à privacidade.

## 3 EFEITOS DA VIOLAÇÃO DA TUTELA À PRIVACIDADE FRENTE AO *BIG DATA* E SEUS DESDOBRAMENTOS E ALTERNATIVAS LEGISLATIVAS DE COMBATE

Como estudado anteriormente, no item 1 do presente artigo, o direito à privacidade protege a vida privada, ou seja, toda manifestação de cunho íntimo e não público de determinado sujeito. Entende-se, assim, por informação privada, toda aquela

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

referente ao modo de viver da pessoa, como os hábitos, desejos, convicções, relacionamentos afetivos e liberdade sexual, ou o que ocorra em seu lar. Entretanto, devido aos avanços tecnológicos, tal proteção ultrapassa o “direito de estar só”, uma vez que, agora, as sensações, emoções e pensamentos ganharam a forma de dados pessoais disponíveis e que circulam facilmente nas redes.

Dessa maneira, é sabido – e comprovado, perante os casos desenvolvidos no item 2 – que o direito à privacidade tem sido posto em xeque diante da circulação de dados pessoais na Sociedade da Informação, impulsionada, sobremaneira, pelas tecnologias de informática e telecomunicações hodiernamente aplicadas nos mais diversos segmentos da vida cotidiana. Fixado isso, como toda ação gera reação, tais medidas de violação, através do acesso a dados pessoais, geram consequências na vida cidadã dos indivíduos.

Como exemplo, o serviço chamado *Spokeo* (*apud* CARLONI, 2013), que atua nos Estados Unidos da América (EUA), utiliza-se do fenômeno do *Big Data* (tratado no item 2.1) como mecanismo para buscas específicas sobre pessoas determinadas, por meio de seu nome, e-mail, telefone, cidade etc. A base de dados disponível no *Spokeo* não é desenvolvida por essa empresa, por meio do rastreamento do usuário, por exemplo. Trata-se de um software de organização de informações, as quais derivam de dados disponíveis publicamente em diversos setores, encontrados em listas telefônicas, redes sociais, pesquisas de marketing, anúncios imobiliários, entre outros.

Segundo a autora, o usuário do *Spokeo*, aquele que realiza a busca, pode ser tanto pessoa física quanto jurídica ou órgão governamental. Caso tal pessoa decida por pagar a mensalidade desse serviço (inferior a US$ 5,00), terá acesso detalhado a uma série de dados pessoais de terceiros, sem que os usuários tenham conhecimento sobre os resultados que podem ser obtidos e, também, sem permitirem esse ingresso em sua vida privada.

Esse sistema de busca através do *Big Data* e do *Deep Packet Inspection* viola uma série de direitos fundamentais previstos na Declaração Universal dos Direitos

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

Humanos (DUDH, 1948), como o artigo XII, que trata sobre a não interferência na vida privada do individuo, sendo essa ação uma clara quebra de privacidade, na medida em que são fornecidos a desconhecidos, de todo o globo, dados pessoais que os particulares nem ao menos consentem na aquisição. Além disso, vê-se uma objetiva comercialização banal de dados privados, visto que são vendidos por menos de US$ 5,00, violando a plena cidadania da pessoa por mera ânsia do poder de possuir a informação.

Além disso, o infeliz caso da *Cambridge Analytica*, em que houve utilização de dados privados, obtidos através do *Facebook,* para permitir predizer e influenciar as escolhas dos eleitores nas urnas por meio de um sistema que deduz a personalidade e as inclinações políticas das pessoas, a partir de seus perfis nessa rede social, comprado pela empresa, comprometeu – além do direito à privacidade – a liberdade sem interferências de escolha de seus representantes políticos, mediante manipulação de informações, o que prejudicou uma formação intelectual verídica sobre os fatos que chegavam na *timeline* e, consequentemente, a cidadania íntegra desses indivíduos que foram violados.

Percebe-se que a realidade proporcionada pelo fenômeno *Big Data* gera implicações sobre a questão da privacidade, que não podem ser ignoradas ou negligenciadas. Logo, faz-se fundamental o estabelecimento de regras e contornos, definições de limites, para que essa realidade gere externalidades positivas e não o que já se tem percebido recentemente, como as práticas denunciadas do *Cambridge Analytica* e as diversas empresas que utilizam do *Deep Packet Inspection* para obtenção de dados para proliferação de propagandas.

Para Celina Silva e Elaine Rodrigues (2017):

> O controle dos processos legais é mandatório, mas deve ser justificado. Se privacidade for definida como requisito essencial para alcance da moralidade, então, privacidade é um direito que a lei deve não só proteger, mas prover.

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

O governo brasileiro, em busca de legislar sobre a temática, a fim de amenizar situações indiscriminadas de quebra do direito à privacidade dos usuários, criou em 2014 a Lei n. 12.965/2014, denominada Marco Civil da Internet, a qual rege normas, deveres, princípios e direitos para a utilização da internet, no país, por usuários, empresas e provedores de internet.

A privacidade é abordada nesta lei no art. 3º e no art. 7º. No texto, afirma-se – mais uma vez – a inviolabilidade da intimidade e da vida privada, bem como a sua proteção e indenização por dano material ou moral decorrente de sua violação. Além disso, no inciso II e III, do art. 7º, dizem que é inviolável o sigilo do fluxo das comunicações pela internet, salvo por ordem judicial, na forma da lei, além da inviolabilidade e sigilo das comunicações privadas armazenadas, salvo por ordem judicial (PLANALTO, 2014).

Segundo Joana Machado (2015), embora a legislação aborde a temática da proteção de dados pessoais, não a faz de maneira detalhada e deixa a tarefa a cargo de posterior lei específica. Dessa forma, o legislador cuidou apenas de alguns aspectos da tutela dos dados pessoais no desenvolvimento desta Lei.

Assim, alterando o Marco Civil da Internet (Lei n. 12.965/2014), foi criada a Lei Geral de Proteção de Dados (n. 13.709 de 2018), a qual estabelece regras de coleta e tratamento de informações de pessoas, empresas e instituições públicas, os direitos de titulares de dados, as responsabilidades de quem processa esses registros, as estruturas e formas de fiscalização e eventuais reparos em caso de abusos nesta prática (VALENTE, 2019).

Nessa medida, propõe a estudada Lei que:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (PLANALTO, 2019)

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

A lei em questão estabelece uma série de regras e obrigações para as empresas e outras organizações atuantes no Brasil seguirem, para possibilitar que o cidadão tenha plena convicção e ciência sobre o tratamento que é dado para suas informações pessoais.

Segundo Luana de Paula (2018), as organizações públicas e privadas só poderão coletar dados pessoais se tiverem consentimento do titular. Tal solicitação deverá ser feita de maneira clara, para que o indivíduo saiba exatamente o que vai ser coletado, para quais fins e se haverá compartilhamento, para que casos como o *Cambridge Analytica* e o abusivo *Deep Packet Inspection* não continuem acontecendo de maneira exaltada.

Assim, de acordo com a autora, quando houver envolvimento de menores, os dados somente poderão ser tratados com o consentimento dos pais ou responsáveis legais, por exemplo. Se houver mudança de finalidade ou repasse de dados a terceiros, um novo consentimento deverá ser solicitado. Além disso, em caso de vazamento de dados, esse fato deverá ser comunicado às autoridades competentes, para que tomem as medidas civis e criminais necessárias.

Desse modo, de acordo com Jonas Valente (2019), a fiscalização ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD) e, como sanção, esse órgão poderá aplicar multas de até 2% do faturamento da empresa (com limite de R$ 50 milhões) e bloqueio ou eliminação dos dados relacionados a uma infração.

Por fim, tendo em vista os fatos tratados, além dos inúmeros outros que podem ser facilmente visualizados em nosso dia-a-dia e as consequências abordadas sobre os casos estudados, vê-se que , em uma sociedade da informação como a atual, em que os dados representam um bem poderoso, apontando-se como representação da própria personalidade do indivíduo, diretrizes são essenciais para versar sobre a temática que terá como principal favorecido o cidadão, titular dos dados pessoais, devendo ser considerado parte mais frágil nas relações que envolvem grandes organizações empresariais e o próprio Estado (MACHADO, 2015). Assim, com a adoção de uma

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

regulação de proteção de dados, o indivíduo passa a ter maior segurança no que diz respeito ao tratamento adequado de tais informações, que compõem sua privacidade e intimidade, assegurando ao cidadão o controle e a titularidade sobre suas próprias informações e garantindo uma cidadania plena.

## CONCLUSÃO

É possível concluir, a partir do exposto, que o direito à privacidade, iniciado por Samuel Dennis Warren e Louis Demitz Brandeis, no denominado “right to privacy”, está positivado mundialmente no ordenamento jurídico  Declaração Universal dos Direitos do Homem (1948), e, nacionalmente, na Constituição Federal de 1988. Todavia, as redes sociais e os sites, através do sistema do *Big Data* e de seus desdobramentos, a exemplo do *Deep Packet Inspection,* embaraça a garantia íntegra desse direito, sendo legítimo comparar esse atual cenário ao panoptismo criado por Jeremy Bentham.

Assim, tendo em vista os argumentos apresentados sobre o assunto *Big Data*, pode-se afirmar que todos os dados que são altamente volumosos e que transitam na rede – seja por meio de redes sociais, GPS, cartão de crédito, compras online etc – são analisados por tal sistema.Tais dados são avaliados de acordo com a frequência de acesso e com o que está sendo visualizado, sendo armazenados para futuro uso.

Dessa maneira, a discussão jurídica em torno da ofensa ao direito à privacidade relaciona-se diretamente com os meios positivos e negativos do acesso às informações e utilização das redes sociais. No aspecto do *Deep Packet Inspection* (DPI), como já foi exposto, podemos frisar a presença do armazenamento para utilização e venda das informações, a fim de um posterior uso para publicidade, havendo um redirecionamento do tráfego de dados, não priorizando um direito fundamental de cada indivíduo, o direito à privacidade.

ISSN 2176 1035 Jornal ELETRÔNICO V. 12, n. 1 - Jan-Jun de 2020
Faculdades Integradas Vianna Júnior

Em vista das mudanças recentes no mundo, o avanço da tecnologia criou um novo cenário, no qual a atuação de leis para a proteção dos direitos se faz necessária. Esta necessidade fica muito clara e evidente no caso *Cambridge Analytica,* dissertado, anteriormente, neste trabalho, cujo panorama mostra como surgiram empresas que lucram ao coletar os dados de diversos usuários da rede, a fim de vendê-los, como, por exemplo, a empresa em questão que colhia as informações privadas dos usuários para a promoção de campanhas políticas.

Por fim, as consequências da violação de dados pessoais, através do *Big Data* e do *Deep Packet Inspection,* tornam-se claras e comprometem direitos fundamentais, a exemplo do estudo do caso da *Cambridge Analytica*. Para evitar que essa atuação anti-ética se perdure e atinja mais indivíduos, o Poder Legislativo brasileiro criou a Lei de Proteção de Dados Pessoais (2018) para a tutela dos cidadãos e consequente sanção àqueles que a violarem. Sendo assim, os indivíduos ficam mais protegidos no que tange à seguridade de seus dados pessoais e à preservação de seus direitos.

## REFERÊNCIAS

ANDRADE, Diogo Queiroz. Cambridge Analytica, a empresa que manipula a democracia à escala global. Disponível em: https://www.publico.pt/2018/03/20/tecnologia/noticia/ca-a-empresa-que-manipula-a-democracia-a-escala-global-1807409. Acesso em: 13 out 2019.

ANDRÉA, G. As redes sociais estão ameaçando a democracia. 14 de agosto de 2019. Acesso em: 26 de outubro de 2019. Disponível em: http://www.justificando.com/2019/08/14/as-redes-sociais-estao-ameacando-a-democracia/

BRASIL. **Constituição Federal de 1988**.

BRASIL. Planalto Lei nº 12.965, de 23 de abril 2014.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Planalto Lei nº 13.709 de Agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

CARLONI, G. Privacidade e Inovação na Era do Big Data. Fundação Getúlio Vargas. Junho de 2013. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/12664/Giovanna%20Louise%20Bodin%20de%20Saint-Ange%20Comn%c3%a8ne%20Carloni.pdf?sequence=1&isAllowed=y

FORTES, Vinicius; MIGLIAVACCA,Luciano. DPI – Deep Packet Inspection: Uma análise da violação da privacidade de e dos dados pessoais no ciberespaço como pratica de transgressão dos direitos humanos a partir da tecnologia de inspeção profunda de pacotes.Disponível em:http://www.publicadireito.com.br/artigos/?cod=5496f40877a2ded2. Acesso em: 28 out 2019.

FREITAS, Thainá. CEO da Cambridge Analytica é suspenso após polêmicas com Facebook e Channel 4, 2018. Disponível em: https://www.startse.com/noticia/nova-economia/tecnologia-inovacao/47764/ceo-da-cambridge-analytica-e-suspenso-apos-polemicas-com-facebook-e-channel-4. Acesso em: 26 out 2019.

GALDINO, Natanael. ´´Big Data: Ferramentas e Aplicabilidade``. Disponível: https://www.aedb.br/seget/arquivos/artigos16/472427.pdf. Acesso: 05 nov 2019.

GUIMÓN, Pablo. Cambridge Analytica, empresa pivô no escândalo do Facebook, é fechada. Disponível em: https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html. Acesso em: 15 out 2019.

JIMÉNEZ, Rosa Cano. Mais de 400 mil brasileiros foram afetados pelo vazamento de dados do Facebook. Disponível em: https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235_618558.html. Acesso em: 15 out 2019.

LOTT, Y; CIANCONI, R. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. Acesso em: 26 de outubro de 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362018000400117

MACHADO, J. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Arquivo Jurídico.** Teresina-PI, v. 2, n. 2, p. 43-65 Jul./Dez. de 2015

NOJIRI, S. O direito à privacidade na era da informática algumas considerações. **Revista jurídica UNIJUS.** Uberaba-MG, V.8, nº 8, p. 99/106, maio 2005. Acesso em: 26 de outubro de 2019. Disponível em: http://www.revistas.uniube.br/index.php/unijus/article/viewFile/1032/1207#page=99

PASSARELLI, Vinícios. LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/. Acesso em: 13 out 2019.

PAULA, L. Breves considerações sobre a lei geral de proteção de dados. 13 de dezembro de 2018. Acesso em: 26 de outubro de 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI292692,71043-Breves+consideracoes+sobre+a+lei+geral+de+protecao+de+dados

PEDROSO, Waldir. Deep Packet Inspection (DPI): o que é e para que serve. IMasters. 2012. Disponível em: https://imasters.com.br/devsecops/deep-packet-inspection-dpi-o-que-e-e-para-que-serve. Acesso em: 28 out 2019.

PETRY, André. ´´O Berço do Big Data``, Revista Veja. Edição 2321, 2013. Disponível: https://lucianabicalho.files.wordpress.com/2013/08/veja-big-data.pdf. Acesso: 05 nov 2019.

PIRES, Alexandre; RALVES, Cláudio. O direito à privacidade frente aos avanços tecnológicos na sociedade da informação. Jus. 2014. Disponível em:https://jus.com.br/artigos/27972/o-direito-a-privacidade-frente-aos-avancos-tecnologicos-na-sociedade-da-informacao. Acesso em: 28 out 2019.

POZZI, Sandro. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. Disponível em: https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html. Acesso em: 13 out 2019.

RONCOLATO, M. O uso ilegal de dados do Facebook pela Cambridge Analytica. 19 de mar de 2018. Acesso em: 26 de outubro de 2019. Disponível em: https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-h%C3%A1-de-novo

SILVA, C.R.;RODRIGUES, E.M.T. “Privacidade em Big Data: panorama e agenda de pesquisa”, Sistemas & Gestão, Vol. 12, No. 4, pp. 491-505,2017. Disponível:http://www.revistasg.uff.br/index.php/sg/article/view/1205/769. Acesso em: 05 nov 2019.

VALENTE, J. Lei de Proteção de dados traz desafios a empresas, cidadãos e governo. Agosto de 2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo

VIEIRA, T. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da tecnologia. Acesso em: 26 de outubro de 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf