

**A ATUAÇÃO DO DIREITO INTERNACIONAL COMO GARANTIDOR DA
PROTEÇÃO DE DADOS E DO DIREITO À PRIVACIDADE: um estudo de caso sobre
o vazamento e manipulação de dados dos usuários do *facebook* pela *cambridge analytica*.¹**

Érica Ângela Lima dos Santos ²

Flávia Kelma Coelho Araújo ²

Rita de Cássia Cardoso Borges ²

Heloísa Gomes Medeiros ³

RESUMO

O presente trabalho apresenta um estudo de caso sobre o *Facebook* e o uso de dados pessoais dos seus usuários pela empresa *Cambridge Analytica* por meio da tecnologia *Big Data*, demonstrando como esta ferramenta de grande utilidade para o alto desempenho de uma organização pode contribuir de forma negativa ao manipular uma pessoa para tomada de decisões. Sendo o indivíduo, um sujeito de direito internacional, fica demonstrada a relevância da proteção de dados pessoais por este ramo do direito, estabelecendo parâmetros para o adequado uso dos dados preservando assim, o direito à privacidade do indivíduo. Por esta razão, o propósito deste trabalho é descrever e qualificar a tecnologia *Big Data*, assim como relatar o caso da manipulação de dados dos usuários do *Facebook* pela *Cambridge Analytica* e como a tecnologia *Big Data* contribuiu para este feito e, por fim, verificar a atuação do Direito Internacional com vistas à proteção dos dados pessoais. O procedimento metodológico adotado é o bibliográfico. O trabalho tem como escopo facilitar a compreensão de procedimentos adotados pelo Direito Internacional afim de evitar a violação, preservando direitos humanos no contexto atual num prisma de sociedade contemporânea cibernética.

Palavras-chave: *Big Data*. *Cambridge Analytica*. *Facebook*. Proteção de Dados Pessoais. Privacidade. Direito Internacional.

1 INTRODUÇÃO

¹ *Paper* apresentado à disciplina Direito Internacional Público, Centro Universitário - UNDB.

² Graduandas do 5º período do Curso de Direito da UNDB – Centro Universitário. Turma DT05AN

³ Professora, Doutora, Orientadora

O Direito Internacional Público surge com o objetivo de regular as ações dos Estados, no âmbito global, criando normas que ultrapassam os limites territoriais de cada um. Após várias evoluções da matéria, observa-se que além dos Estados, os Organismos Internacionais e, mais recentemente, os Indivíduos são sujeitos de direito internacional.

Ao analisar o indivíduo como sujeito de direito internacional, levando em consideração a atual conjuntura da globalização, mediante novas tecnologias, e a possibilidade deste indivíduo ultrapassar os limites dos Estados por meio da rede de computadores, faz-se necessário a regulamentação do uso de dados pessoais desses indivíduos, no sentido de garantir a proteção de direitos individuais, como a privacidade e todos os outros direitos decorrentes dela, assim como a dignidade da pessoa humana. Para tanto, se torna indispensável a atuação dos Estados e Organismos Internacionais para o alcance de tal objetivo.

Tal proteção se torna imperiosa com vistas a vários eventos ocorridos pelo mundo sobre o vazamento de dados pessoais feito por grandes empresas, seja para garantir cliente, mercado, vendas entre outras possibilidades. Tem-se como exemplo *Cambridge Analytica*, que fora acusada de manipulação de dados dos usuários do *Facebook* em corridas eleitorais.

Desta forma se faz o questionamento: o direito internacional público deve atuar em favor do alcance da proteção de dados pessoais mediante a padronização internacional do direito à informação com vistas ao direito de privacidade?

Ora, não cabe ao direito ditar os modos como a tecnologia deve operar, imputando qualquer tipo de determinação que atrapalhe o desenvolvimento tecnológico pois um dos objetivos do armazenamento dos dados pessoais por parte de empresas é estabelecer perfis individuais, observando o que é relevante ou não para determinada pessoa, individualizando produtos e/ou serviços, preferências, por meio de uma publicidade e propaganda direcionadas.

No entanto, diante da globalização, se faz cogente a atuação do direito como protetor dos dados pessoais, na finalidade de evitar a utilização desordenada destas informações, como foi o caso da manipulação de dados dos usuários da rede social *Facebook*. Desta forma o direito internacional deve sim desempenhar o papel de garantidor da proteção de dados pessoais dos indivíduos no exercício da liberdade de expressão com o objetivo de impedir a violação ao seu direito à privacidade.

A sociedade contemporânea está cada vez mais dependente do uso da internet no seu dia a dia, seja para a realização de tarefas ou para a interação social, porém pouco se pensa nos resquícios de dados pessoais que ficam retidos na rede e como esta informação poderá ser empregada. Por se tratar de um comportamento que transpassa os limites territoriais de um país e como o indivíduo é um dos sujeitos do direito internacional público, cabe a este ramo do

direito regulamentar as ações destinadas à proteção dos dados pessoais em virtude dos direitos da pessoa humana.

No estudo que será apresentado, no que tange o âmbito acadêmico, o presente trabalho elenca assuntos relevantes na esfera do Direito Internacional Público e tem por análise um estudo de caso sobre como foi possível o uso e manipulação de dados pessoais dos usuários da rede social *facebook*, pela empresa *Cambridge Analytica*.

No campo social a escolha do tema se deve como uma forma de alertar a sociedade sobre a importância das informações deixadas em rede, numa plataforma digital por exemplo, diante de manifestação positiva na aceitação dos termos e condições de uso de sites. Por fim, pessoalmente, o tema é muito interessante por trazer o amadurecimento acadêmico ampliando a gama de conhecimento aprimorando o senso crítico inerente ao cotidiano das pesquisas científicas.

A metodologia diz respeito aos procedimentos que serão adotados para a realização de um trabalho definindo o tipo de pesquisa e como será aplicada. Sendo assim, o *paper* em questão utiliza como metodologia a pesquisa bibliográfica com levantamento de conteúdos substanciais, de relevante importância, servindo de base teórica para amparar a presente pesquisa com o objetivo de solucionar o problema proposto. Gil (2010) afirma que a pesquisa bibliográfica objetiva a busca de solução do problema a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e, atualmente, material disponibilizado na internet. Então, materiais disponíveis em internet assim como livros e artigos periódicos serão a base deste trabalho.

A razão deste trabalho acadêmico está em descrever e qualificar a tecnologia *Big Data*, assim como relatar o caso do vazamento e manipulação de dados dos usuários do *Facebook* pela *Cambridge Analytica* e como a tecnologia *Big Data* contribuiu para este feito e, por fim, verificar a atuação do Direito Internacional com vistas à proteção dos dados pessoais objetivando o resguardo ao direito de privacidade.

2 BIG DATA COMO FERRAMENTA DE COLETA DE DADOS

Big Data é o vocábulo utilizado pela área de conhecimento Tecnologia da Informação que aborda sobre o processamento e armazenamento de dados grandes, volumosos, rápidos e complexos. Este termo foi utilizado primeiramente no início do século XXI por astrônomos e geneticistas, quando a memória dos computadores já não suportava o armazenamento de grande quantidade de informação disponível levando-os a novas formas e

instrumentos para a análise dos gigantes bancos de dados (SZINVELSKI; ARCENO; FRANCISCO, 2019, p. 8).

Tais autores afirmam que a função do *Big Data* é:

Essencialmente, de analisar o comportamento social, emocional e informacional do consumidor, logo, o intuito maior dessas tecnologias é gerar lucros de maneira exponencial e aumentar a capacidade de atuação do universo empresarial na sociedade, mediante informações que são emanadas pelas pessoas e não somente de maneira verbal, mas física e intelectual. (SZINVELSKI; ARCENO; FRANCISCO, 2018, p.8)

Para Silveira, Marcolin e Freitas (2015) trata-se de um recurso hodierno com vistas ao tratamento de grandes volumes de dados úteis para posterior utilização no intuito de direcionar a gestão de tomadas de decisões nas organizações. Cabe ressaltar a importância desta ferramenta para a vida moderna ao fornecer dado, informação e conhecimento possibilitando o desenvolvimento da empresa e, conseqüentemente, da sociedade. (apud SANTOS; CAMILO; MELO, 2018, p. 52)

A ferramenta em questão está pautada em qualidades que os especialistas chamam de 5V's: valor, volume, velocidade, variedade e veracidade. 1) valor se refere no investir da empresa em melhoria da qualidade dos serviços para que haja retorno e o aumento de sua receita; 2) volume é a grande quantidade de dados gerado; 3) velocidade é o gerenciamento dinâmico destas informações, pois se assim não for, perde seu valor; 4) variedade é a capacidade de vários canais tem de produzir dados como os e-mails, **mídias sociais** entre outros; 5) veracidade porque os dados precisam ser reais. (FIORIO, 2014)

Não há dúvidas quanto ao potencial desta ferramenta para grandes empresas e para benefício da população em geral, pois por meio do *Big Data*, além de gerenciar dados é possível gerar riquezas uma vez que “as sociedades que mais lucram [...] são aquelas que gerenciam informação.” (FLORIDI, 2016 apud NERDOLOGIA, 2016).

Segundo Fiorio (2014), “um dos segmentos que mais pode se valer do *Big Data* é o da publicidade, sendo possível se comunicar com os mais distintos grupos, apenas pelo fato de conhecer os seus desejos, saber quais são os seus sonhos e preferências.” Assim, o *Big Data* se transforma em instrumento capaz de possibilitar uma vantagem competitiva para fins políticos ou comerciais possibilitando a personalização e difusão de mensagens em termos de indivíduo ou de grupo específico quando o usuário tem milhares de dados a seu respeito sendo coletados, organizados, relacionados e analisados continuamente, criando-se, então, a oportunidade de lhe transmitir mensagens que sejam mais precisas (BIMBER, 2014 apud CALDAS; CALDAS, 2019, p. 202)

Como já dito, os dados coletados são oriundos de diversas fontes, entre elas estão as redes sociais. Por meio delas houve um aumento vertiginoso de dados onde qualquer indivíduo passou a criar grande quantidade de conteúdo uma vez que o usuário deixa suas marcas nestas plataformas ao compartilhar o que se consumiu, por onde se passou, o que se assistiu ou leu, as novas amizades, entre tantas outras atividades do dia-a-dia. O *Facebook* é um exemplo de rede social onde há grande capacidade de coleta de dados pessoais deixados por seus usuários, desta forma:

São 300 milhões de fotos subidas diariamente e já existe capacidade de processamento para “mastigar” esses dados e saber muita coisa. Através de quem são seus amigos e de onde você estudou o *facebook* pode sugerir quem foram seus colegas no colégio. Através de quem aparece nas mesmas fotos que você e com reconhecimento facial se sabe com quem estava. Juntando ainda os dados de interesses quando se curte, música que se escuta, as relações podem ser ainda mais reveladoras. (NERDOLOGIA, 2015)

Conforme demonstrado o indivíduo não apenas gera ou transmite informação. Ele é capaz de processar os dados. Isto posto, o *Big Data* tornou-se assim um “método de rastreamento das preferências humanas afim de auxiliar no planejamento estratégico dos grandes setores empresariais” (SANTOS; CAMILO; MELO, 2018, p. 58). A questão é como utilizar esses dados coletados, por meio da tecnologia *Big Data*, de uma forma ética, que não transgrida direitos individuais.

A coleta de dados, mediante o *Big Data*, dos sujeitos que utilizam a internet evidencia o desenvolvimento das ciências e economia, mas esses dados podem ser utilizados de forma errônea com objetivos escusos gerando consequências inesperadas/indesejadas por parte da população (CALDAS; CALDAS, 2019, p. 200). Foi exatamente o que se percebeu no caso dos usuários da plataforma *Facebook* quando se evidenciou a prática ilícita do uso de dados pessoais dos seus usuários pela empresa *Cambridge Analytica*, ocorrendo, sob a ótica do direito, a violação ao direito humano de privacidade.

3 A MANIPULAÇÃO DE DADOS PESSOAIS DOS USUÁRIOS DO FACEBOOK POR MEIO DA CAMBRIDGE ANALYTICA

Relacionando *Big Data*, política e eleições é possível inferir que dados pessoais dos usuários de redes sociais “já são utilizadas como ferramentas eleitorais há pelo menos seis anos” (CALDAS; CALDAS, 2019, p. 202).

Exemplo mais recente desta afirmativa é o caso da empresa *Cambridge Analytica* que usou dados dos usuários da plataforma de interação social *Facebook* por intermédio do *Big*

Data, para fins eleitorais. Se trata de uma empresa, com sede na Inglaterra, fundada em 2013, voltada para serviços nas áreas comerciais e de consultoria política realizando-os por meio de análise de dados. Além da Inglaterra, sua atuação ocorria nos Estados Unidos, Malásia e, inclusive, Brasil.

A análise de dados é legal. A título de exemplo, no Brasil há jurisprudência firmada, conforme súmula 550 do Superior Tribunal de Justiça, no entendimento de que é possível o uso de dados de consumidores para fins financeiros. É o *score* de crédito. Segundo Lupion (2015, p. 432) *score* de crédito é o resultado sistêmico dos hábitos de pagamento e relacionamento do cidadão com o mercado de crédito criado por pessoa jurídica que tem o **controle de bancos de dados, coleta, armazenamento e análise** em que atribuem pontuações como que uma bonificação para pessoas que honram seus compromissos financeiros, servindo de base para a decisão de concessão de crédito. Em se tratado de análise de dados para fins políticos, também não há problema desde que seja por um método envolto de legalidade. O que não pode ocorrer são artifícios obscuros para o uso desses dados, de forma eivada de ilegalidade.

A aplicabilidade indiscriminada dos dados dos usuários do *Facebook* ocorreu a partir do uso de um aplicativo desenvolvido por um professor de psicologia russo, Aleksandr Kogan, acerca de teste de personalidade com fulcro acadêmico com perguntas e respostas. Assim o *Facebook* o autorizou a usar a plataforma. Para realizar o teste, o usuário permitia a coleta de dados: identidade, localização, gostos pessoais e contatos de seus amigos. Isso corrobora a falta de rigor no controle de dados pelo *Facebook* dos seus usuários.

Os dados foram vendidos à *Cambridge Analytica*. A empresa adquiriu “dados sensíveis de cerca de 87 milhões de usuários [...] a maioria não havia dado permissão” (STROUD, 2018). A empresa atuava “atingindo uma massa de indivíduos com publicidade especialmente direcionada a eles” (ANASTASIA, 2019, p. 165). Uma publicidade baseada nas informações fornecidas de forma inocente pelos usuários da rede social.

O site *naçõesunidas.org* fez uma analogia ao comparar os dados dos usuários a *commodities* pois seus hábitos de busca, compras, opiniões políticas e redes de amigos foram analisados e vendidos para obtenção de lucro.

De acordo com Court Stroud da Revista *Forbes* a *Cambridge Analytica* atuava da seguinte forma:

A empresa percebeu como colocar dados do usuário para enganar consumidores - sobre produtos, candidatos, ideias políticas - usando a *Big Data* para empreender campanhas de propaganda que, na verdade, não desempenhava nenhum papel, mas com a intenção de coletar dados para desenvolver o perfil de personalidade - gostos, desgostos, pontos de vista sobre várias questões sociais - e, a partir desse perfil, poder

testar palavras e frases para ver quais reações elas gerariam. Palavras e frases que provocam fortes reações tornam-se os botões quentes nas mensagens da campanha. Assim, se você inundar a internet com mensagens suficientes, poderá alterar o resultado de uma eleição. (STROUD, 2018, tradução nossa) ^[1]

A principal publicidade era voltada para a área política. Na época da campanha eleitoral dos EUA em 2016, a *Cambridge Analytica* “manipulava, manchando candidatos com notícias fabricadas, a fim de mudar o rumo das eleições para os candidatos que ela favorecesse - política suja. [...]” (STROUD, 2018)

Essas “notícias fabricadas” se referem a *fake news*. Normalmente, o objetivo de uma *fake news* é criar uma polêmica em torno de uma situação ou pessoa, contribuindo para o denegrimento da sua imagem. Por ter um teor extremamente dramático, apelativo e polêmico, as *fake news* costumam atrair muita atenção das massas, principalmente quando estas estão desprovidas de senso crítico. Assim, os conteúdos falsos podem agir como uma "arma" ilegal contra algo. No âmbito político, por exemplo, as notícias falsas são usadas com o intuito de "manchar" a reputação de determinado candidato, fazendo com que perca potenciais eleitores. (NOVO, 2018)

Apenas para título de informação ao leitor, as notícias falsas se espalham 70% mais rápido que as verdadeiras e alcançam muito mais gente. A conclusão é do maior estudo já realizado sobre a disseminação de notícias falsas na internet, concretizado por cientistas do MIT (Instituto de Tecnologia de Massachusetts), nos Estados Unidos publicado na revista *Science*. (NOVO, 2018)

E como direcionar a exata notícia falsa? Por meio do acesso ilícito a dados pessoais do indivíduo. Quando este deixava a sua marca na rede como gosto, preferências, por exemplo, era possível direcionar a “adequada” mensagem pré-fabricada para ele, por meio da tecnologia *Big Data*. Caldas, Caldas (2019, p. 198) aludem:

A eleição para a presidência dos Estados Unidos da América (EUA) que deu a vitória a Donald Trump se tornou emblemática, pois ficou marcada pelas revelações a respeito da utilização – de maneira irregular – de análise de dados de usuários do *Facebook* para promover estratégias de campanha eleitoral e ataques a adversários, sobretudo, à candidata Hillary Clinton. Esse episódio gerou apreensão e expectativas, especialmente, nos países nos quais existem eleições livres e acentuado uso de Internet por parte dos cidadãos.

^[1] The firm saw how it could put user data to work to mislead consumers, be it about products, candidates, political ideas—using big data to wage propaganda campaigns in which truth played no role. Its founding premise: If you gathered enough data on a person, you could then develop a personality profile—likes, dislikes, views on various social issues— and from that profile you could then test words and phrases to see what reactions they generated. Words and phrases that drew strong reactions became the hot buttons in campaign messages. If you flooded the internet with enough such messages, you could change the outcome of an election.

Foram as investigações que demonstraram a influência dessa tecnologia nas urnas. Robôs e *Big Data* mapeavam o perfil dos eleitores, que a *Cambridge Analytica* detinha os dados, no sentido de adaptar o discurso do candidato conforme o perfil, para conquistar a simpatia desse eleitor até conseguir o seu voto.

Dessa maneira “ficou evidenciado a participação desta empresa na campanha presidencial de Donald Trump do ano de 2016. Os usuários do *Facebook* foram manipulados através de publicidade na rede para, de tal forma, beneficiar determinado candidato. ” (ANASTASIA; LARA, 2019, p. 165)

Comprovado o uso do *Big Data* para a manipulação de dados a ponto de favorecer determinado candidato em épocas de eleição, é reativada a discussão sobre a necessidade de normatizar o uso de tecnologias com vistas à proteção de direitos fundamentais como o da privacidade e, conseqüentemente, a proteção de dados pessoais.

4 A ATUAÇÃO DO DIREITO INTERNACIONAL NA PROTEÇÃO DOS DADOS PESSOAIS

A tecnologia desempenha evidente papel na modernização da sociedade, sendo possível o seu acesso mediante o uso da internet, conectando pessoas do mundo inteiro. Mas o uso da internet deixa rastros. Pessoas, ao utilizá-la, fornecem todo tipo de dados pessoais que ficam disponíveis a quem souber usá-los. Desta forma, o escândalo do uso de dados pessoais indiscriminados dos usuários do *Facebook* pela *Cambridge Analytica*, a necessidade de proteção de dados voltou a ser tema de debate no mundo todo.

O acesso aos dados pessoais sem a devida permissão dos usuários configura violação ao direito de privacidade, previsto no artigo 12 da Declaração Universal dos Direitos Humanos. Se trata de um direito que representa “uma ‘porta de entrada’ a dados pessoais e que reforça outros direitos, online e offline, incluindo o direito à igualdade e não discriminação, liberdade de expressão, de reunião [...]”. (BRASIL, 2018).

A privacidade é um direito essencial à proteção da dignidade humana com o objetivo de proteção contra interferências não autorizadas na vida do sujeito de direito que acabariam por influenciar a sua forma de interagir com o mundo. A privacidade limita quem tem acesso aos corpos, lugares e coisas, assim como as comunicações e informações do indivíduo. (BRASIL, 2018). Mas é fato que o setor público e privado recolhe cada vez mais os dados pessoais dos indivíduos.

Apesar do direito à proteção de dados não estar expresso no rol de direitos humanos, há uma tendência de reconhecê-lo com tal. Danilo Doneda (2011, p. 96) afirma:

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.

O que se percebe é que tudo era muito recente, e ainda é, quando se fala em tecnologia. Sampaio (1997) destaca:

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado dessa tecnologia, sem que se soubesse ao certo suas consequências, fez com que se optasse por princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados, além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados. Esse enfoque era natural, visto a motivação dessas leis ter sido a “ameaça” representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática de tais leis eram algo tecnocrático e condicionado pela informática – nelas, tratavam-se dos “bancos de dados”, e não propriamente da “privacidade”, desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo. (apud DONEDA, 2011)

Apesar de não estar no rol que prevê direitos humanos, a Corte Europeia de Direitos Humanos reconheceu a proteção de dados pessoais como um direito fundamental. Esse entendimento foi alicerçado quando julgou o caso *Big Brother Watch v. the U.K.*, cujo o americano Edward Snowden, que atuava junto à NSA, revelou ações do governo norte-americano que monitoravam não apenas alvos intencionais, mas também pessoas comuns e estes representavam 90% do quantitativo total de pessoas que sofreram com interceptação nas comunicações. A decisão da Corte foi baseada no artigo que trata do direito à privacidade, o 8º.

A *Cambridge Analytica* ainda está sob investigação, mas o que ocorreu tem “potencial para demonstrar uma ligação ainda maior entre a proteção de dados pessoais, direitos humanos e democracia, visto que as informações pessoais de diversos usuários do *Facebook* foram usadas para guiar campanhas político-partidárias.” (FICO; MOTA, 2020). A *Cambridge Analytica* em 2018 fechou, iniciando o processo de falência, primeiro na Inglaterra e depois nos Estados Unidos.

Com o escândalo da *Cambridge Analytica* fica demonstrada a vulnerabilidade das ações do *Facebook* na forma de tratar os dados pessoais dos seus usuários. O escândalo vai além, quando a ferramenta utilizada para a manipulação desses dados foi o *Big Data*, uma

solução para empresas em organizar grande volume de dados dos seus clientes, que tem por objetivo a potencialização de um negócio.

Recentemente, Mark Zuckerberg, um dos fundadores do *Facebook*, foi chamado perante a corte americana para esclarecimentos. Em depoimento ele falou que a plataforma é uma ferramenta poderosa, que conecta pessoas, mas reconheceu que não fizeram o suficiente para proteger os dados dos seus usuários que sofreram com “*fake news*, interferência estrangeira nas eleições, discursos de ódio, assim como desenvolvedores e privacidades dos dados. Não tivemos uma visão ampla da nossa responsabilidade [...] vai levar um tempo para fazer as mudanças necessárias, mas eu me comprometo a corrigir tudo.” (DEPOIS DA VERDADE, 2020)

Há pouco tempo, o *Facebook* atualizou sua política de Termos de Uso e Privacidade. Nos Estados Unidos, a empresa foi autuada a pagar cinco bilhões de dólares e a Inglaterra, devido à violação da Lei de Proteção de Dados, foi multado, pela Autoridade Nacional Inglesa – ICO - que representa a autoridade de proteção de dados, em cerca de quinhentas mil libras esterlinas (HERN; PEGG, 2018 apud PINHEIRO, 2018, p 28)

Dentre as legislações que regulamentam a proteção de dados a nível de blocos mundiais, existe a *General Data Protection Regularion*, - GDPR - em vigor desde maio de 2018, que reforça os direitos dos cidadãos e tornam mais compreensíveis as regras para as empresas na era digital. Versa sobre a proteção de dados pessoais dos cidadãos da União Europeia, empresas do mundo que negociam com países da UE, garantindo a privacidade de dados, estabelecendo parâmetros de atuação para as empresas, com previsão de advertências para aquelas que não cumprem o estabelecido e, também, direitos que beneficiam cidadãos como:

Um consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a ser esquecido — um cidadão pode solicitar que os seus dados sejam suprimidos; o direito a transferir os dados para outro prestador de serviços (por exemplo, a mudança de uma rede social para outra); e o direito de saber se os seus dados foram pirateados. (PARLAMENTO EUROPEU, 2020)

O parlamento europeu trata a proteção de dados pessoais e o respeito à privacidade como direitos fundamentais. Assim, “o Parlamento Europeu sempre insistiu na necessidade de alcançar um equilíbrio entre as melhorias da segurança e a preservação dos direitos humanos, incluindo a privacidade e proteção de dados.” (PARLAMENTO EUROPEU, 2020)

No sentido de proteger os dados dos usuários de internet, países do mundo inteiro estão cada vez mais atuantes na elaboração de legislações que definam os limites de atuação

das empresas no que se refere a armazenamento, tratamento e manipulação de dados, pois entendem a necessidade de proteção de dados pessoais dos indivíduos. Entre outros países pelo mundo, se tem, a nível de América Latina, a Argentina, o Chile, a Colômbia, o México e o Brasil. Este último a lei ainda não entrou em vigor.

Conforme explica Ignacio Ybáñez, embaixador da União Europeia no Brasil, a proteção de dados pessoais é fundamental para o crescimento econômico dos países. Por exemplo, a GDPR trouxe benefícios aos países europeus, pois estabeleceu padrões para a proteção dos dados pessoais, responsabilizando as empresas que violam esse direito humano e conscientizando os cidadãos de seus direitos. Ele também afirma que legislações referentes à proteção dos dados pessoais no contexto global, devem ser padronizadas facilitando o fluxo internacional de dados, permitindo acordos que vislumbrem o respeito à privacidade do indivíduo e, por conseguinte, facilitando o fluxo livre de dados pessoais. Neste sentido, com a padronização, seria mais fácil, inclusive, um acordo entre o Mercosul e a União Europeia. (BERBET, 2019)

A tendência para o tratamento adequado e proteção de dados pessoais é tão grande que se tornou necessária a regulamentação no ordenamento interno dos países que querem estabelecer acordos comerciais com os países da União Europeia, por exemplo.

5 CONSIDERAÇÕES FINAIS

O intuito do trabalho foi demonstrar a necessidade de proteção aos dados pessoais dos indivíduos, em âmbito digital, pelo direito internacional, pois se tratam de sujeitos de direito internacional e, desta forma, há a necessidade de proteção aos direitos inerentes ao homem como o da privacidade e as suas ramificações. Para a concretização deste objetivo, utilizou-se do emblemático caso do *Facebook* e como a política de proteção de dados pessoais dos usuários era vulnerável e inadequada, o que permitiu o vazamento e manipulação dos dados pessoais dos usuários pela *Cambridge Analytica* por meio da tecnologia *Big Data*.

Sendo assim, no primeiro tópico, partindo da necessidade e modernização eficaz dos meios de armazenamento de volumosos dados nas organizações, foi descrita a tecnologia *Big Data* como ferramenta de coleta de dados de usuários no meio digital, nas diversas possibilidades de uso oferecidas pelas organizações, permitindo a elas mais êxito no seu gerenciamento de negócios pois esta ferramenta possibilita uma coordenação das informações, que são emanadas pelas próprias pessoas, de forma consentida. Assim, com o *Big Data* a

empresa dispõe de uma carteira de clientes, com a exata informação de qual produto, serviço, publicidade e propaganda direcionar ao usuário, pois detém arquivos com seus dados pessoais.

Em seguida, foi versado o caso do vazamento de dados pessoais dos usuários do *Facebook*, pela empresa de consultoria política *Cambridge Analytica* que manipulou os dados pessoais com a ferramenta *Big Data*. Questionou-se o comprometimento e responsabilidade do *Facebook* na política de proteção de dados pessoais dos seus usuários e a forma fraudulenta com que a *Cambridge Analytica* fez uso dos dados pessoais dos usuários, ao direcionar notícias pré-fabricadas sobre pessoas que estavam concorrendo à eleição no ano de 2016 no Estados Unidos, o que acabou por influenciar opiniões e decisões individuais, especulando-se o nível de interferência que este ato representou no resultado da eleição democrática deste Estado.

Por fim, abordou-se a atuação do direito internacional na proteção dos dados pessoais e, por conseguinte, o direito de privacidade, pois como o indivíduo é sujeito de direito internacional, cabe a este ramo do direito definir diretrizes afim de proteger indivíduos e responsabilizar as organizações quando há o vazamento de dados pessoais, como o caso exposto, principalmente quando envolve objetivos escusos. O papel do direito internacional não é impossibilitar o uso e desenvolvimento de tecnologias para o fomento econômico, mas torná-la adequada ao que o mundo contemporâneo requer, com clareza, para que o indivíduo seja capaz de desfrutar do livre exercício do seu direito de privacidade e com a devida proteção aos seus dados pessoais, usufruindo das benesses oferecidas pelo mundo digital.

REFERÊNCIAS

BERBET, Lúcia. **Autoridade independente é destacada em audiência sobre proteção de dados**. 2019. Disponível em: <http://www.telesintese.com.br/autoridade-independente-e-destacada-em-audiencia-sobre-protecao-de-dados/>. Acesso em: 24 maio 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial Submetido à Sistemática Prevista no Art. 543-c do CPC. Ação Cautelar de Exibição de Documentos. Crediscor n° 1.304.736. Relator: Ministro Luis Felipe Salomão. Rio Grande do Sul de 2016. **Recurso Especial**. Rio Grande do Sul, 24 fev. 2016.

BRASIL, Nações Unidas. **Artigo 12: Direito à privacidade**. 2018. Disponível em: <https://nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acesso em: 24 maio 2020.

CALDAS, Camilo Onoda Luiz; CALDAS, Pedro Neres Luiz. Estado, democracia e tecnologia: conflitos políticos e vulnerabilidade no contexto do big-data, das fake news e das shitstorms. **Perspectivas em Ciência da Informação**, São Paulo, v. 24, n. 2, p.196-220, 15 abr. 2019. Trimestral.

CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 5., 2019, Santa Maria. **Big Data e Proteção de Dados: Uma Relação Possível (?)**. Santa Maria: Ufsm, 2019. 15 p. Disponível em: <file:///C:/Users/Edgar%20Santos/Desktop/Érica%20Ângela/Concurso/Curso%20Direito/5º%20Período/Direito%20Internacional%20Público/Big%20Data%20e%20a%20proteção%20de%20dados.pdf>. Acesso em: 12 abr. 2020.

DEPOIS da Verdade: **Desinformação e o Custo das Fake News**. Direção: Andrew Rossi. Nova Iorque: HBO, 2020. 1 DVD (95 min.).

EUROPEU, Parlamento. **Proteção dos Dados Pessoais**. 2020. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais>. Acesso em: 20 abr. 2020.

FICO, Bernardo de Souza Dantas; MOTA, Juliana da Cunha. **A proteção de dados como direito humano**. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-como-direito-humano-29022020>. Acesso em: 20 abr. 2020.

FIORIO, Vivian. **O que é Big Data e para que serve?** 2014. Disponível em: <https://industria hoje.com.br/o-que-e-big-data-e-para-que-serve>. Acesso em: 12 abr. 2020.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010. 184p.

LUPION, Ricardo. O caso do sistema de "credit scoring" do cadastro positivo. **Revista da Ajuris**, Rio Grande do Sul, v. 42, n. 137, p.431-449, mar. 2015.

NERDOLOGIA. **Big Data**. 2015. Disponível em:
<https://www.youtube.com/watch?v=hEFFCKxYbKM&t=184s>. Acesso em: 12 abr. 2020.

MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: Uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Estado de Direito e Tecnologia**: Edição Temática, Vitória, v. 19, n. 3, p.159-180, set. 2018.

NERDOLOGIA. **Dilúvio de dados**. 2016. Disponível em:
<https://www.youtube.com/watch?v=pNZq8BCS-Bc&t=225s>. Acesso em: 12 abr. 2020

NOVO, Benigno Nuñez. **Fake news e o direito**. 2018. Disponível em:
<<https://jus.com.br/artigos/64666/fake-news-e-o-direito>>. Acesso em: 24 mai. 2020.

PORTELA, Paulo Henrique Gonçalves. **Direito Internacional Público e Privado**. 4. ed. Salvador: Juspodium, 2012. 512 p.

SANTOS, Beatriz Rosa Pinheiro dos; CAMILO, Ewerton da Silva; MELLO, Mariana Rodrigues Gomes de. Big Data e Inteligência Artificial: Aspectos Éticos e Legais mediante Teoria Crítica. **Rev. Fil. Tem**, Belém, v. 1, n. 3, p.50-61, 15 jan. 2018. Semestral.

STROUD, Court. **How The Struggle Over The Use And Abuse Of Consumers' Data Could Play Out**. 2018. Disponível em:
<https://www.forbes.com/sites/courtstroud/2018/04/29/how-the-struggle-over-the-use-and-abuse-of-consumers-data-could-play-out/#3c4eaa3b45bc>. Acesso em: 03 mar. 2020.

VITTORIA ALVARES ANASTÁSIA, 4., 2019, Rio Grande do Norte. **O Escândalo Cambridge Analytica: A manipulação de dados na era digital**. Rio Grande do Norte: Percurso, 2019. 3 p.