



CENTRO UNIVERSITÁRIO SANTA AMÉLIA – UNISECAL
BACHARELADO EM DIREITO

AMANDA BONETTE

RESPONSABILIDADE CIVIL NO USO DA INTERNET

PONTA GROSSA

2020



AMANDA BONETTE

A RESPONSABILIDADE CIVIL NO USO DA INTERNET

**Artigo apresentado como critério de avaliação da
Disciplina de Trabalho de Curso II, 9º Período A, do
Curso de Bacharelado em Direito do Centro
Universitário Santa Amélia – UniSecal.**

Orientadora: JulyanaNeiverth

PONTA GROSSA

2020

CURSO DE BACHARELADO EM DIREITO
TERMO DE AUTORIZAÇÃO DE DEPÓSITO DO ARTIGO

Eu, professora JULYANA NEIVERTH autorizo o depósito e defesa do artigo intitulado
RESPONSABILIDADE CIVIL NO USO DA INTERNET do acadêmico/a AMANDA THAÍS
BONETTE.

Ponta Grossa, 26 de novembro de 2020.


Assinatura Professor/a

*Dedico esse artigo a Deus, por ter sido meu companheiro
fiel todos os dias e por ter honrado meu esforço.*

AGRADECIMENTOS

Agradeço primeiramente a Deus pela vida maravilhosa que me proporciona, cheia de aprendizado e oportunidades de crescimento. Agradeço pela vida que estou com as pessoas que estou, eu me sinto extremamente abençoada todos os dias.

À minha mãe por ser a pessoa que mais admiro no mundo, meu porto seguro. Você é a mulher com o coração mais bondoso que já conheci, se eu me tornar ao menos um pouco do que você é nesta vida serei uma mulher realizada.

Ao meu filho, tão amado, que veio de presente durante esses anos de graduação pra me dar forças e pra me mostrar o quanto capaz eu sou para realizar meus sonhos e correr atrás dos meus objetivos, pois desde que você chegou aprendi o significado do amor incondicional.

Ao meu pai por ser um homem admirável, exemplo de força e sabedoria pra minha vida.

Aos meus avós que já se foram em vida, mas que continuam presentes todos os dias de minha vida em minhas lembranças, acredito que estão orgulhosos.

Às minhas tias, tios e primos, às crianças de minha vida, por serem meu refúgio em dias difíceis. A inocência de vocês é a coisa mais bonita e pura que existe. Minha família é o maior presente que eu poderia ter recebido em minha vida.

Às minhas poucas, mas verdadeiras amigas que mesmo não tendo parentesco sanguíneo se incluem em minha família, sempre confiaram em meu potencial. Obrigada por cada ombro amigo, cada palavra de conforto e incentivo, vocês são a força de todos os dias de minha vida.

Aos professores que compartilharam toda sua sabedoria nestes cinco anos juntos. Principalmente a minha professora-orientadora Julyana Neiverth e minha professora da matéria do TC II Adriana Mello, as quais eu tenho grande admiração não apenas como profissional, mas como ser humano, por toda paciência, disponibilidade e compreensão, vocês fizeram desde então parte de uma das etapas mais importantes de minha vida. Sorte a minha ter sido escolhida por vocês para me orientar.

RESPONSABILIDADE CIVIL NO USO DA INTERNET

Amanda Thais Bonette (Centro Universitário UniSecal)
Julyana Neiverth (Centro Universitário UniSecal)

Resumo: Nos dias de hoje a internet se tornou a tecnologia mais avançada e com mais velocidade para comunicação, aumentando a preocupação em se garantir direitos fundamentais da população. Dada a atualidade da temática o presente trabalho objetiva analisar o direito à privacidade e sua relação com a proteção de dados a partir da análise do caso concreto do *Facebook VS Cambridge Analytica*. Para isto, foram traçados os seguintes objetivos: analisar a responsabilidade civil em atos praticados na internet; apresentar e descrever a legislação brasileira que abarca questões relacionadas ao direito de privacidade e proteção de dados, inclusive na internet; contextualizar e analisar o caso *Facebook VS Cambridge Analytica*. O estudo de caso (*Facebook VS Cambridge Analytica*), sob o viés do direito à privacidade no Brasil, envolveu aspectos jurisprudenciais e legislativos, sob o prisma da Constituição Federal de 1988 (CF), do Código de Defesa do Consumidor (CDC) (Lei nº 8.078/90), do Código Civil (Lei nº 10.406/02), do Marco Civil da Internet (Lei nº 12.965/14), e da Lei Geral de Proteção de Dados Pessoais (LGPD) (Leis nº 13.709/18 e 13.853/19). Embora o caso tenha ocorrido nos Estados Unidos, também foi possível verificar o vazamento de dados de usuários brasileiros, de modo que o *Facebook* foi processado no Brasil, no ano de 2018, pelo Departamento de Proteção e Defesa do Consumidor. À época, havendo descumprimento ao Código de Defesa do Consumidor e ao Marco Civil da Internet, bem como dano aos usuários afetados, reconheceu-se o nexo de causalidade e o *Facebook* foi condenado. Neste caso, houve a imposição de sanção administrativa na forma de multa, no valor de seis milhões e seiscentos mil reais para o Facebook. A proteção de dados, decorrente do direito à privacidade encontra respaldo técnico na responsabilidade civil, também aplicada a atos ilícitos e ilegais praticados na internet.

Palavras-chave: *Facebook*. *Cambridge Analytica*. Privacidade. Proteção de dados. Jurisprudência.

CIVIL RESPONSIBILITY IN THE USE OF THE INTERNET

Abstract: Nowadays the internet has become the most advanced technology and with the highest speed for communication, increasing the concern to guarantee fundamental rights of the population. Given the topicality of the theme, the present work aims to analyze the right to privacy and its relationship with data protection from the analysis of the specific case of Facebook VS Cambridge Analytica. For this, the following objectives were outlined: to analyze civil liability in acts performed on the internet; present and describe the Brazilian legislation covering issues related to the right to privacy and data protection, including on the internet; contextualize and analyze the Facebook VS Cambridge Analytica case. The case study (*Facebook VS Cambridge Analytica*), under the bias of the right to privacy in Brazil, involved jurisprudential and legislative aspects, under the prism of the Federal Constitution of 1988 (CF), of the Consumer Protection Code (CDC) (Law 8,078 / 90), the Civil Code (Law 10,406 / 02), the Civil Marco de Internet (Law 12,965 / 14), and the General Personal Data Protection Law (LGPD) (Laws 13,709 / 18 and 13,853 / 19). Although the case occurred in the United States, it was also possible to verify the leakage of data from Brazilian users, so that Facebook was sued in Brazil, in 2018, by the Department of Consumer Protection and Defense. At the time, with noncompliance with the Consumer Protection Code and the Internet Civil Framework, as well as damage to affected users, the causal link was recognized and Facebook was condemned. In this case, an administrative sanction was imposed in the form of a fine of six million and six hundred thousand reais for Facebook. Data protection, resulting from the right to privacy, finds technical support in civil liability, also applied to illicit and illegal acts practiced on the internet.

Keywords: Facebook. Cambridge Analytica. Privacy. Data protection. Jurisprudence.

1 INTRODUÇÃO

Nos dias de hoje a internet se tornou a tecnologia mais utilizada e com maior velocidade de comunicação, expandindo opiniões sobre diversos temas, culturas, pessoas, informações. Por meio de aparelhos celulares e computadores, é possível acessar redes sociais de qualquer lugar do mundo em frações de segundos. A internet é vista como um dos maiores marcos da “globalização”, com isso se tornou necessário olhar sob o viés da proteção aos direitos fundamentais para os casos de atos ilícitos ocorridos na internet.

Com o uso da internet, vem à preocupação em se garantir direitos fundamentais, como a privacidade, direito de sons e imagens, proteção de dados, liberdade de expressão, inviolabilidade da intimidade, consentimento livre e esclarecido para divulgação de dados pessoais, e assim por diante.

Atualmente, temos algumas leis que merecem destaque sobre o tema: a primeira é a Constituição Federal de 1988 (CF), que prevê o direito à inviolabilidade da vida privada, honra, intimidade e imagem de toda a população brasileira. Depois, temos o Código de Defesa do Consumidor (CDC) (Lei nº 8.078/1990), que rege a legislação consumerista nacional e prevê a proteção contra publicidade enganosa e abusiva.

Na sequência, a Lei 12.965/2014, também conhecida como Marco Civil da Internet, regulamentou o serviço da internet, como a garantia da liberdade de expressão na “internet” e em “redes sociais” (Artigo 2º, Artigo 8º e Artigo 19), e o direito de privacidade de cada usuário (Artigo 2º, Artigo 8º e Artigo 11). Um dos aspectos desta lei se refere à definição das responsabilidades dos provedores de internet e aplicativos, visando regular os atos praticados via internet.

Posteriormente, entrou em vigor a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018), que regulamentou o tratamento de dados pessoais, visando proteger os direitos de privacidade e liberdade, inclusive em meio digital. Esta lei foi alterada no ano seguinte pela Lei nº 13.853/2018, a qual criou a Autoridade Nacional de Proteção de Dados (ANPD), que é responsável, nos termos da legislação, proteger os dados pessoais.

Dada a atualidade da temática, o presente artigo possui como objetivo analisar o direito à privacidade e sua relação com a proteção de dados a partir da análise do caso concreto do *Facebook VS Cambridge Analytica*.

Para isso, foram traçados os seguintes objetivos específicos: analisar a responsabilidade civil em atos praticados na internet; apresentar e descrever a legislação

brasileira que abarcar questões relacionadas ao direito de privacidade e proteção de dados, inclusive na internet; contextualizar e analisar o caso *Facebook VS Cambridge Analytica*.

2 DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

Atualmente, a partir do advento das Tecnologias de Informação e Comunicação (TIC), as pessoas passaram a ter acesso a todos os tipos de informação de maneira prática e facilitada. Por meio da *internet* houve ampliação da comunicação com pessoas que se encontram distante, acesso a informações, notícias, materiais acadêmicos, e assim por diante. São inúmeras as variedades de: “sítios onde é possível conversar com outras pessoas, divulgar pensamentos ou informações de trabalhos realizados, são disto exemplos os *blogs*, os *chats*, o correio eletrônico, as redes sociais, tal como, o *Hi5* ou o *Facebook*, entre outras” (PIRES; NOVO; GOMES, 2010, p. 83).

Apesar de serem inúmeros os aspectos positivos do advento das TIC, há aspectos negativos que trazem riscos por conta de ilegalidades e abusos em sua utilização (PIRES; NOVO; GOMES, 2010), principalmente no que tange à privacidade e proteção de dados. De acordo com Pires, Novo e Gomes (2010, p. 83), em algumas destas ferramentas “as informações tornam-se públicas e qualquer pessoa pode ter acesso e utilizar do modo menos correto”.

É importante salientar que nestes sítios digitais, as pessoas precisam concordar em tornar suas informações públicas, uma vez que o direito à privacidade se encontra normatizado no ordenamento jurídico. Desta forma, neste capítulo foi abordado sobre o direito à privacidade e proteção de dados, bem como sobre a responsabilidade civil.

A cada dia cresce muito os negócios relacionados à internet; vivemos a era da comunicação, em que informações são repassadas em frações de segundos revolucionando de uma maneira muito abrangente a internet. A internet nos dias de hoje é um dos principais meios de comunicação, utilizada também para concessão de negócios, de atos jurídicos, trazendo a necessidade de tornar essas relações via internet numa ótica jurídica.

A internet foi criada nos Estados Unidos no final da década de 1960 e início da década de 1970 (meados da guerra fria), a partir de projetos relacionados à necessidade de mais segurança no armazenamento de informações e modos mais eficazes de salvaguardar e compartilhar com maior velocidade e alcance os mesmos (OLIVEIRA, 2014). Preto e Pinto (2006) descrevem seu surgimento:

Departamento de Defesa dos Estados Unidos, durante a guerra fria, que, ao solicitar à Advanced Research Projects Agency (ARPA) uma rede de computadores capaz de continuar funcionando na ausência de um nó ou quebra de uma conexão, deu

origem, em 1969, à rede Internet (ISOC, 2000), que se constitui na chamada *rede das redes* (PRETO; PINTO, 2006, p. 20).

No Brasil, as primeiras redes de comunicação de dados utilizavam redes telefônicas ou de telex, sendo que as primeiras linhas de transmissão digital surgiram em 1976, com a instalação da EMBRATEL entre os estados de São Paulo e Rio de Janeiro (AGUIAR, 2001 *apud* CARVALHO, 2006). Na década de 1980 foi implantado, pela TELESP, o videotexto, que consistia em uma tecnologia que “permitia ao usuário do sistema telefônico conectar um aparelho adaptador especial e receber informações diversas em uma televisão comum” (CARVALHO, 2006, p. 67).

Foi apenas na década de 1990 que houve a implantação da Internet no Brasil, promovendo “grande incentivo à criação de redes internas nas instituições, através da integração das redes locais antes isoladas” (CARVALHO, 2006, p. 99). A partir de 1996 o acesso à internet foi disseminado no país e “seguiu seu caminho rumo à popularização” (CARVALHO, 2006, p. 124).

Na atualidade o comércio eletrônico está avançando cada vez mais em todo o mundo. A internet encontra-se presente em celulares, televisores – não apenas aquela rede mundial de computadores como era na época, possibilitando um acesso a informação e interatividade muito mais ampla e eficaz. Assim, existem as vantagens e desvantagens referidas ao tema, sendo questões que atraem o ordenamento jurídico e afetam o consumidor que se cadastra em plataformas e aplicativos via internet. De acordo com Pinheiro (2013, p. 47):

[...] há pouco mais de quarenta anos, a Internet não passava de um projeto, o termo “globalização” não havia sido cunhado e a transmissão de dados por fibra óptica não existia. Informação era um item caro, pouco acessível e centralizado. O cotidiano do mundo jurídico resumia-se a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. Essa nova era traz transformações em vários segmentos da sociedade – não apenas transformações tecnológicas, mas mudanças de conceitos, métodos de trabalho e estruturas. O Direito também é influenciado por essa nova realidade. A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana.

De acordo com o mesmo autor, “toda mudança tecnológica é uma mudança social, comportamental, portanto, jurídica” (PINHEIRO, 2013, p. 49). Assim deve o Direito acompanhar a evolução da tecnologia presente na geração da internet. Ou seja, o Direito deve se adaptar e solucionar, visando normas e princípios, buscando pacificar o convívio social, uma vez que existem muitos indivíduos que usam a internet com o intuito de praticar delitos das mais variadas espécies, causando danos e prejuízos, que necessitam de reparação.

No que concerne o ordenamento jurídico brasileiro, conforme já citada, a Lei nº 12.965/14, além de abordar sobre o uso da internet no país, determinou as “diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios” (BRASIL, 2014, artigo 1º).

Um dos princípios do uso da internet no Brasil é a “garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal” (BRASIL, 2014, artigo 3º, inciso I). Além deste princípio, outros dois se destacam neste mesmo artigo: “II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei” (BRASIL, 2014, artigo 3º, incisos II e III). Ou seja, apesar de os usuários e provedores de internet possuírem liberdade para se comunicar, se expressar e manifestar suas opiniões, deve ser respeitada e garantida a proteção dos dados pessoais, bem como o direito à privacidade.

No que diz respeito às empresas provedoras de internet e a proteção dos dados pessoais, de acordo com o inciso VII do artigo 7º da Lei nº 12.965/14, seus contratantes (usuários) encontram-se assegurados ao seguinte direito: “não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei” (BRASIL, 2014, artigo 7º, inciso VII).

Na seção II desta lei foi disposto especificamente sobre a proteção dos registros, dos dados pessoais e das comunicações privadas (BRASIL, 2014). Assim, a guarda e disponibilidade de registros na internet “devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas” (BRASIL, 2014, artigo 10). Havendo infração por parte dos provedores de internet, as sanções serão aplicadas da seguinte forma, de acordo com o Artigo 12 da Lei: advertência; multa; suspensão temporária e/ou proibição das atividades (BRASIL, 2014), sendo que os mesmos não serão “responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros” (BRASIL, 2014, artigo 18). Questões relacionadas aos provedores de internet e sua responsabilidade civil foram abarcadas no tópico a seguir.

2.1 PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET

A privacidade pode ser definida como a faculdade de cada indivíduo em impedir a intromissão de estranhos em sua vida familiar e pessoal, bem como de impedir o acesso e divulgação de suas informações particulares e privadas (BASTOS, 1989 *apud* VIEIRA, 2007). Ao ampliar para o conceito de “direito à privacidade”, Pereira (2004 *apud* VIEIRA, 2007, p. 23) define o como: “poder das pessoas de controlar suas informações pessoais, as

quais, ainda que não formem parte da vida privada das mesmas, passam a revelar aspectos de sua personalidade”.

“O direito à privacidade como figura jurídica autônoma é construção recente que tem reconhecido seu marco inicial, geralmente, no trabalho realizado por Warren e Brandeis” (CANCELIER, 2017, p. 217), em 1890. Este direito nasceu em berço burguês, permanecendo “restrito às suas origens até o final da primeira metade do século XX” (CANCELIER, 2017, p. 219). Esta realidade começou a ser alterada apenas na década de 1960, “motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da tecnologia” (CANCELIER, 2017, p. 219).

Na legislação brasileira, destaca-se que o termo “privacidade” não foi abarcado na Constituição Federal de 1988 (BRASIL, 1988) e no Código Civil de 2002 (BRASIL, 2002), sendo utilizados outros termos, como vida privada, sigilo, intimidade, segredo, inviolabilidade (CANCELIER, 2017; OLIVEIRA; BARROS; PEREIRA, 2017). Apesar de o constituinte ter optado pelo uso de outros termos, “no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, o direito à privacidade é considerado direito fundamental e direito da personalidade” (CANCELIER, 2017, p. 222).

De acordo com a Constituição Federal, “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, artigo 5º, inciso X). Ou seja, quando infringido o direito à privacidade, a pessoa violada possui direito à indenização, tanto por danos morais como materiais.

Em âmbito internacional, o “direito estadunidense prevê o *righttoprivacy*” (GARCIA, 2018, p. 6), não fazendo distinção entre intimidade e privacidade, havendo proximidade com o ordenamento brasileiro. Conforme já exposto, independentemente do modo com que o termo é designado no ordenamento brasileiro e internacional, a privacidade é um “componente essencial à formação da pessoa, indispensável à construção do indivíduo e de suas fronteiras com os demais” (DONEDA, 2008 *apud* CANCELIER, 2017, p. 223). Neste sentido, Cancelier (2017, p. 223) completa ao afirmar que “sua tutela vai ao encontro da promoção e proteção da dignidade da pessoa humana, fundamento norteador do nosso ordenamento jurídico”.

Tendo em vista o advento das TIC, atualmente também se fala em direito à “privacidade *online*” (OLIVEIRA; BARROS; PEREIRA, 2017, p. 568). Nesta perspectiva, o conceito de liberdade evoluiu do “direito de estar só para direito a ter controle sobre as próprias informações e de determinar a maneira de construir a própria esfera particular – o

direito à autodeterminação informativa” (PEIXOTO JUNIOR, 2016, p. 358). Assim, a função política e social da privacidade extrapola os limites da esfera privada, constituindo-se, também, em cidadania (PEIXOTO JUNIOR).

Levando-se em consideração os riscos de invasão à vida privada e intimidade por meio dos novos recursos tecnológicos, bem como da divulgação ilegal de informações, é de suma importância falar sobre a proteção de dados na internet. Na sociedade da informação, os dados pessoais das pessoas encontram-se inseridos em arquivos e sistemas informatizados desde seu nascimento (VIEIRA, 2007). Sobre isto Vieira (2007, p. 225-226) descreve:

Desde o nascimento, o indivíduo já tem inseridos os respectivos dados pessoais em arquivos informatizados da Secretaria de Registro Civil. Ao longo dos anos, passa a integrar também os arquivos da Secretaria de Segurança Pública, do Conselho Nacional de Trânsito, da Receita Federal, dos conselhos profissionais e outros. Isto sem mencionar os registros de estabelecimentos médicos, de instituições financeiras, de estabelecimentos de ensino, de associações, de lojas, de bibliotecas e de tantos outros estabelecimentos. Essas informações, uma vez coletadas, são armazenadas em bancos de dados ligados em rede, o que permite a interconexão dos arquivos e a definição do perfil de seus titulares, medida que se consuma em alta velocidade, com baixo custo e com pequena margem de erro.

A partir da interconexão destes dados, a qual pode ser realizada por meio de inúmeros *softwares* de busca e cruzamento de informações, há possibilidade de se criar um perfil de determinada pessoa, sem sua autorização, e até sem seu conhecimento, tanto para fins públicos como privados (SILVA, 2020; VIEIRA, 2007). Além da inserção de dados em registros públicos, as pessoas podem inseri-los em plataformas online, como bancos e redes sociais, sendo que estes dados devem ser protegidos contra divulgação ilegal e não autorizada.

Isto se deve ao fato de que, o tratamento e vazamento de dados pessoais podem causar graves danos a seus titulares. Além da invasão de privacidade, caso o indivíduo não possua conhecimento da existência dos bancos de dados, há inviabilização de “correção de dados incorretos, incompletos e defasados” (VIEIRA, 2007, p. 228).

Com relação ao ordenamento jurídico brasileiro, é importante destacar três leis que abarcam questões referentes ao uso da internet e proteção de dados. Com o avanço tecnológico e ascensão da internet, no ano de 2014 foi regulamentada a Lei nº 12.965/14 a Lei nº 12.965/14 (Marco Civil da Internet), estabelecendo “princípios, garantias, direitos e deveres para o uso da Internet no Brasil” (BRASIL, 2014). Esta lei foi apresentada e discutida no capítulo 2.

Quatro anos mais tarde foi sancionada a Lei nº 13.709/18, a qual, além de alterar o Marco Civil da Internet, dispôs 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” (BRASIL, 2018a, artigo 1º). De acordo o artigo 2º da referida lei, a proteção de dados encontra-se regida pela liberdade de expressão; respeito à privacidade, intimidade e honra; direito de imagem; independência informativa e livre iniciativa; defesa do consumidos; respeito aos direitos humanos (BRASIL, 2018a).

Percebe-se, portanto, que a proteção de dados se encontra respaldada no respeito à privacidade, direito à liberdade de expressão, direito aos direitos humanos, dignidade e exercício da cidadania, além de visar à garantia da inviolabilidade da imagem, da intimidade e, conseqüentemente, da honra. Além de apresentar estes fundamentos, a Lei nº 13.709/18 ainda traz conceitos como dado pessoal¹, dado pessoal sensível², dado anonimizado³ e banco de dados⁴, conforme os seguintes incisos do artigo 5º. Esses conceitos são relevantes porque demonstram que independente da origem e convicção do dado ou de que forma encontra-se armazenado, todos são passíveis de proteção, garantindo o direito à privacidade.

No ano de 2019, esta lei foi alterada pela Lei nº 13.709/19, passando a ser conhecida como Lei Geral da Proteção de Dados Pessoais (LGPD). Visando a proteção dos dados, foi criada a “Autoridade Nacional de Proteção de Dados (ANPD)” (BRASIL, 2019, artigo 55A), a qual é composta pelo Conselho Diretor (composto por, no máximo, cinco diretores); Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (composto por 23 representantes, titulares e suplentes); corregedoria; ouvidoria; órgão de assentamento jurídico; unidades administrativas e unidades especializadas (BRASIL, 2018a). O que permite inferir uma preocupação estatal com a fiscalização do uso de dados pessoais.

Em casos em que ocorrer invasão de privacidade ou não proteção de dados, há mecanismos de defesa e proteção que os titulares podem recorrer, dentre os quais se destacam a autotutela e o habeas data.

A autotutela tem por base a proteção dos dados realizada pelo próprio indivíduo, realizada por meio da cautela e divulgação do mínimo possível de informações e dados pessoais na web (LEONARDI, 2012; OLIVEIRA; BARROS; PEREIRA, 2017). Já o habeas data é um importante instrumento jurídico constitucional, que garante o “direito de acessar os registros existentes em bancos de dados e em cadastros de consumo, bem como retificar ou

¹I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

²II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

³ III dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

⁴IV banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico [...] (BRASIL, 2018, artigo 5º).

apagar registros errôneos e complementar registros insuficientes ou incompletos” (OLIVEIRA; BARROS; PEREIRA, 2017, p. 578-579).

A legislação prevê alguns princípios específicos que devem ser observados (artigo 6º), como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e prestação de contas (BRASIL, 2018a). Durante este tratamento, o controlador e o operador devem manter registro das operações realizadas, além de dever adotar, de acordo com o artigo 46 da supracitada lei, “medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” (BRASIL, 2018a, artigo 46).

Caso os agentes de tratamento de dados cometam infrações, ficam sujeitos a sanções administrativas⁵. O julgador poderá arbitrar indenizações por dano moral no caso de violação à legislação de proteção de dados, devendo sempre “agir com ponderação, fixando quantia razoável, tendo em vista que um valor ínfimo representaria verdadeiro incentivo ao ato ilícito e que um extremamente elevado implicaria enriquecimento sem causa” (LEONARDI, 2012, p. 224).

3 RESPONSABILIDADE CIVIL

Vinda do Latim *spondeo*, a palavra responsabilidade se vincula ao devedor, ao causador, traz a ideia de restauração de equilíbrio, reparação de danos, devendo ele ser reparado com a ocorrência do fato e a verificação de seus requisitos (GONÇALVES, 2017). A noção jurídica de responsabilidade civil “pressupõe a atividade danosa de alguém que, atuando a priori ilicitamente, viola uma norma jurídica preexistente (legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar)” (GAGLIANO; PAMPLONA FILHO, 2012, p. 54).

A responsabilidade civil se decompõe nos seguintes elementos: “a) conduta humana (positiva ou negativa); b) dano ou prejuízo; c) o nexo de causalidade” (GAGLIANO; PAMPLONA FILHO, 2012, p. 74).

⁵I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples[...]; III - multa diária [...]; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; [...] X - suspensão parcial do funcionamento do banco de dados a que se refere a infração [...]; XI - suspensão do exercício da atividade de tratamento dos dados [...]; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018, artigo 52).

A conduta humana é “guiada pela vontade do agente, que desemboca no dano ou prejuízo” (GAGLIANO; PAMPLONA FILHO, 2012, p. 874), ou seja, é uma conduta voluntária, resultante do direito de liberdade escolha do agente, o qual possui consciência e discernimento do que faz. Sendo classificada em positiva e negativa, destaca-se que a primeira ocorre por meio de uma prática ativa e a segunda por um ato de omissão (GAGLIANO; PAMPLONA FILHO, 2012).

O dano ou prejuízo pode ser conceituado como a “lesão a um interesse jurídico tutelado — patrimonial ou não —, causado por ação ou omissão do sujeito infrator” (GAGLIANO; PAMPLONA FILHO, 2012, p. 88), sendo dividido em dano patrimonial e dano moral. Havendo certeza do dano, o indivíduo lesado possui direito à reparação, a título de compensação, defendendo cumprir os requisitos mínimos para indenização: “a) a violação de um interesse jurídico — patrimonial ou moral; b) a efetividade ou certeza; c) subsistência” (GAGLIANO; PAMPLONA FILHO, 2012, p. 92).

Finalmente, o nexos de causalidade trata-se “do elo etiológico, do liame, que une a conduta do agente (positiva ou negativa) ao dano” (GAGLIANO; PAMPLONA FILHO, 2012, p. 151). Para que se possa concluir pela responsabilidade jurídica do agente infrator, a análise deste nexos se faz indispensável (autor). Ora, por óbvio, “somente se poderá responsabilizar alguém cujo comportamento houvesse dado causa ao prejuízo” (GAGLIANO; PAMPLONA FILHO, 2012, p. 151).

Nos dias de hoje a responsabilidade se torna presente em múltiplas atividades humanas, abrangem o ramo do Direito e invadem os limites da vida jurídica para assim se conciliar em todos os modelos de vida social. A doutrina classifica a responsabilidade civil como um fenômeno social, muito presente no dia a dia, a qual pode ser: violada tanto de normas morais como jurídicas, o fato configura a infração que pode ser proibida pela lei moral, como pela religiosa ou a do Direito (GONÇALVES, 2017). Sobre isto, o autor completa:

O homem sente-se moralmente responsável perante sua consciência ou perante Deus, conforme seja ou não religioso, mas não há nenhuma preocupação com a existência de prejuízo a terceiro. Como a responsabilidade moral é confinada à consciência ou ao pecado, e não se exterioriza socialmente, não tem repercussão na ordem jurídica. Pressupõe, porém, o livre-arbítrio e a consciência da obrigação (GONÇALVES, 2017, p. 12).

Para melhor compreensão, a responsabilidade que não é jurídica traz efeitos na consciência do indivíduo, o qual se sente responsável moralmente por violar princípios, sendo contrária aos efeitos advindos da responsabilidade jurídica, qual é ocasionada pelos

descumprimentos de obrigações e de negócios jurídicos (GONÇALVES, 2017). Importante frisar, de fato, que a responsabilidade do descumprimento de obrigações somente causa efeito após o descumprimento do dever jurídico. Pinheiro (2013, p. 411) completa ao afirmar que:

Em primeiro lugar, a responsabilidade é um fenômeno social. Para o Direito, um dos principais pressupostos da responsabilidade civil é a existência de nexos causal entre o ato e o dano por ele produzido. Muito mais importante que o ato ilícito que causou o dano é o fato de que esse ato deve ser ressarcido.

A responsabilidade civil torna-se muito importante, por dirigir-se à restauração de um dano causado. Segundo o ensinamento de Venosa (2020, p. 1) “toda atividade que acarreta prejuízo gera responsabilidade ou dever de indenizar”. É nesse sentido que o Direito deve analisar a responsabilidade civil perante a sociedade, já que com novas mudanças surgem novas questões jurídicas, a qual o Direito deve se adaptar, visando solucionar normas e princípios.

Apesar da responsabilidade na maioria das vezes aparecer como um descumprimento de obrigação, ela pode aparecer mesmo que não exista nenhum dever, como a obrigação, pode existir sem que haja responsabilidade.

A obrigação nasce de diversas fontes e deve ser cumprida livre e espontaneamente, quando tal não ocorre e sobrevém o inadimplemento, surge a responsabilidade. Não se confundem, pois, a obrigação e responsabilidade. Está só surge se o devedor não cumpre espontaneamente a primeira. A Responsabilidade é, pois, a consequência jurídica patrimonial do descumprimento da relação obrigacional. (GONÇALVES, 2012, p. 20).

Assim, a responsabilidade parte de um dano causado a outra pessoa, a fim de reparar o lesado. Farias, Rosenvald e Netto (2015, p. 6) acrescentam que “o caminho percorrido pela maior parte dos estudiosos do direito civil é o de abrir espaços para a responsabilidade independente da culpa”. Visando um equilíbrio na vida social, principalmente em relações virtuais onde milhares de pessoas se relacionam, ou ainda efetuam vários tipos de serviços e atividades via internet, a responsabilidade civil ganha grande destaque, por isso, a doutrina classifica como um grande fenômeno social.

4 FACEBOOKVSCAMBRIDGEANALYTICA: CONTEXTUALIANDO O CASO

A *Cambridge Analytica* (C.A) foi fundada no ano de 2013 e decretou falência em 2018 (FORNASIER; BECK, 2020). Era uma “empresa privada, filial do grupo SCL (*Strategic Communication Laboratories*), gerida por Nigel Oakes” (GATTI, 2017 *apud* PINHEIRO, 2018, p. 25). Sua atuação ocorria, principalmente, em áreas militares, “sendo financiada e aplicada em setores de contrainteligência e propaganda para mídia e eleitorado”

(PINHEIRO, 2018, p. 25). Para seu funcionamento, era feita uma matemática “a partir da mineração de dados junto à análise estratégica de comunicação para o processo eleitoral” (PINHEIRO, 2018, p. 25), participando de diversas campanhas políticas.

No ano de 2013 Michal Kosinski, inventou a “análise comportamental a partir da curtida no *Facebook* utilizado pela C.A” (PINHEIRO, 2018, p. 25). Tendo conhecimento acerca disto, a C.A contratou pesquisadores da universidade de *Cambridge* para utilizar este método, colocando “em prática o modelo baseado na psicografia semelhante àquela que Kosinski estruturou seus estudos” (GRASSEGGER; KROGERUS, 2017 *apud* PINHEIRO, 2018, p. 27).

Este método era capaz de deduzir diversos aspectos com alta precisão, dentre os quais se destaca a orientação à filiação partidária dentro da plataforma *Facebook*. Seu funcionamento ocorria da seguinte maneira: a partir dos dados básicos e pessoais de cada indivíduo, como locais que frequentam, marcas que utilizam, produtos que adquirem, crenças, religiões, e assim por diante, era possível traçar um padrão e perfil comportamental de cada pessoa.

A partir deste padrão, identificava-se os eleitores mais e menos propensos a votarem em determinado candidato, criando mensagens que se encaixassem em seu perfil (PINHEIRO, 2018). Com este método, no ano de 2013 a empresa C.A disponibilizou um aplicativo (*Quiz* de perguntas) vinculado ao *Facebook*, criado pelo pesquisador Aleksandr Kogan, buscando traçar o perfil de seus usuários, com o intuito de traçar um perfil de pensamento (SERRA, 2018).

Assim, de forma intencional, a empresa fazia uso do *Facebook* para a prática de divulgação de “notícias falsas (*Fake News*) para manipular tendências políticas de eleitores, resultando em uma ruptura da democracia e gerando, de forma deliberada, uma sociedade polarizada” (FORNASIER; BECK, 2020, p. 184).

No ano de 2016, os dados dos usuários do *Facebook* que realizaram este *Quiz* foram utilizados para promover a campanha eleitora do então candidato à presidente dos Estados Unidos, Donald Trump (SERRA, 2018). Estando este perfil político traçado, a C.A foi capaz de “direcionar de forma mais eficaz as propagandas e divulgações de campanha, a fim de abranger o maior número de eleitores possível durante a campanha eleitoral de Donald Trump, o que por consequência geraria um número maior de votos ao final da corrida presidencial” (WENDT JÚNIOR; EHRHARDT; SILVA, 2019, p. 3-4).

Esta prática foi denunciada inúmeras vezes, tanto antes como após a política eleitoral de Donald Trump, com destaque para: Jornalista Harry Davies, em 2015, no jornal inglês *The*

Guardian; jornalistas Hannes Grasseger e Mikael Krogeru, em 2016, no periódico suíço *Das Magazin*; publicação em 2017 na revista *Vice*; Jornalista Carole Cadwalladr, em 2017, no *The Observer* (FORNASIER; BECK, 2020). Nesta época (2017), a C.A sentiu-se ameaçada e “ajuizou ações de responsabilidade civil e criminal por difamação ante os dois jornais e a jornalista, como tentativa de silenciar as investigações” (FORNASIER; BECK, 2020, p. 184). Contudo, “Cadwalladr enfrentou a CA ao – de forma incansável – buscar o maior apoio na comunidade jornalística mundial possível ao seu alcance” (FORNASIER; BECK, 2020, p. 20). Finalmente, no dia 17 de Março de 2018, o destino da C.A foi selado para sempre da seguinte forma:

Nesse dia, três grandes organizações de periódicos e jornais do mundo – *The Observer*, *The Guardian* e *The New York Times* – publicaram em conjunto, simultaneamente, o artigo intitulado *How Trump Consultants Exploited the Facebook Data of Millions* (“Como os consultores de Trump exploraram os dados do Facebook de milhões”). O artigo somente foi viável após muito convencimento, por parte de Carole Cadwalladr, de demonstrar o caminho certo, ético e democrático – apesar de ter um enorme custo pessoal – de sua fonte anônima publicamente denunciar a CA de (i) suas práticas de mineração de dados (*Data Mining*) e tratamento de dados (interpreta-se aqui como a prática de *Data Scraping*) e (ii) interferir de forma eficiente nos resultados de processos democráticos (BERGHEL, 2018 *apud* FORNASIER; BECK, 2020, p. 185).

No caso, é importante ressaltar que a fonte até então anônima da jornalista Carole Cadwalladr era um ex-funcionário da C.A, chamado Christopher Wylie, o qual possuía provas das acusações feitas sobre a empresa, uma vez que antes de sua demissão “levou de forma discreta e cuidadosa cerca 84 milhões de dados pessoais e centenas de arquivos confidenciais da CA” (FORNASIER; BECK, 2020, p. 185). Como este não havia sido um caso isolado da empresa, posteriormente, “Brittany Kaiser, analista de dados sênior da CA, também resolveu aderir à postura adotada por Wylie e se apresentou, de forma voluntária, para depor no Reino Unido contra a CA” (FORNASIER; BECK, 2020, p. 186).

Em primeiro de Maio de 2018 a C.A decretou falência após “ação penal por violação da aplicação das Leis do Escritório do Comissário de Informação do Reino Unido” (PINHEIRO, 2018, p. 28-29) e encontra-se sob sigilo e investigação judicial até os dias de hoje (FORNASIER; BECK, 2020). No que tange à plataforma *Facebook* outras medidas foram tomadas: atualização de “sua política de Termos de Uso e Privacidade, além de ser multado em cerca de 500 mil libras esterlinas por violação da Lei de Proteção de Dados” (HERN; PEGG, 2018 *apud* PINHEIRO, 2018, p. 28).

Por conta do “escândalo” causado por toda esta situação, Mark Zuckerberg (CEO da empresa), de modo a buscar reconquistar a confiança de seus usuários, se comprometeu a:

(i) investigar todos os aplicativos da plataforma; (ii) avisar usuários vítimas de aplicativos abusivos; (iii) restringir o acesso dos desenvolvedores a dados; (iv) reduzir os dados que aplicativos obtêm com logins; e (v) garantir que os usuários entendam quais aplicativos estão autorizados a acessar seus dados (ZUCKERBERG, 2018 *apud* SERRA, 2018, p. 43).

Vale ressaltar que a plataforma do *Facebook* não foi acessada de forma não autorizada, ou seja, não foi invadida. O que ocorreu é que a *Cambridge Analytica* encontrou e utilizou uma “brecha nas normas da política de privacidade dessa rede social para acessar dados de mais pessoas do que as que realmente foram suas usuárias, havendo, posteriormente, o compartilhamento desses dados com outra empresa (não parceira do *Facebook*)” (SERRA, 2018, p. 43).

5 ANÁLISE DO CASO

O presente caso começou a ser investigado em 04 de abril de 2018, no qual havia informações de que usuários do *Facebook* poderiam ter sofrido com o uso indevido de dados pela *Cambridge Analytica*. Segundo a rede social, 87 milhões de pessoas foram atingidas e tiveram suas informações compartilhadas pela consultoria de marketing político, sendo 70 milhões nos Estados Unidos e 443 mil no Brasil (SEI 6156620)⁶.

A empresa de consultoria política *Cambridge Analytica*, conforme análise, usou uma ferramenta capaz de elaborar perfis psicológicos de usuários por meio de suas interações no *Facebook*, a *Big Data*. De acordo com Rubinstein, o *Big Data* é o “instrumento mais poderoso para descobrir conhecimento em base de dados – em outras palavras, ela é apta a obter informações potenciais úteis, previamente desconhecidas e extraídas de forma implícita” (SERRA, 2018, p. 21).

Há evidências de que, com apenas algumas curtidas, o algoritmo do aplicativo é capaz de decifrar o tipo de pessoa que você é (PRIMI, 2018). Levando-se em consideração que todos os dias são compartilhadas postagens no *Facebook*, as quais geram inúmeras curtidas, a partir da técnica descrita é possível levantar e armazenar dados de milhares de pessoas. Portanto, esta ferramenta é aplicada para diversas finalidades, como questões econômicas, políticas, saúde pública, endereçar propagandas para públicos específicos (SERRA, 2018).

No ano de 2013 a *Cambridge Analytica* (C.A) vinculou à plataforma do *Facebook* um aplicativo chamado “*thisisyour digital life*”, coletando informações acerca da

⁶BRASIL. Ministério da Justiça e Segurança Pública. **Processo nº 08012.000723/2018-19**. Representante: Departamento de Proteção e Defesa do Consumidor – exofficio. Representados: *Facebook Inc.* e *Facebook Serviços Online do Brasil Ltda.* Brasília, 04 de Abril de 2018.

personalidade dos usuários, traçando seu perfil político, com o intuito de direcionar, com um método mais eficaz, as propagandas e divulgações de campanha. Assim, foi possível “abranger o maior número de eleitores possível durante a campanha eleitoral de Donald Trump, o que por consequência geraria um número maior de votos ao final da corrida presidencial” (WENDT JÚNIOR; EHRHARDT; SILVA, 2019, p. 3-4). Por exemplo, uma das bandeiras defendidas por Trump era o direito ao porte de arma nos Estados Unidos, sugerindo que armas é uma ferramenta essencial para proteção. Portanto, o anúncio transmitia a mensagem de que as pessoas precisam se proteger de ameaças externas.

No caso em tela, o aplicativo da C.A abusou de uma brecha nas normas da política de privacidade do *Facebook*, para acessar os dados de pessoas que foram suas usuárias, havendo assim, o compartilhamento de tais dados com outra empresa, que não era parceira da rede social (SERRA, 2018). Este vazamento de dados trouxe inúmeros transtornos e complicações para Mark Zuckerberg, dono (e criador) do *Facebook*, “acarretando sua intimidação para prestar esclarecimentos ao Congresso Nacional dos Estados Unidos, com o intuito de explicar o que efetivamente havia ocorrido” (WENDT JÚNIOR; EHRHARDT; SILVA, 2019, p. 4).

Por conta disto, *Facebook* se comprometeu a investigar todos os aplicativos com grande acesso e volumes de informações, conduzindo, inclusive, auditorias completas nos que fossem considerados suspeitos, além de adotar medidas de proteção, alterando suas políticas de privacidade, buscando “resguardar os dados pessoais de seus usuários” (WENDT JÚNIOR; EHRHARDT; SILVA, 2019, p. 4).

No Brasil, no ano de 2018 o caso passou por um processo judicial⁷, em que o Departamento de Proteção e Defesa do Consumidor (DPCD) denunciou o *Facebook Inc.* e o *Facebook Serviços Online do Brasil Ltda.*, com a finalidade de averiguar os fatos ocorridos nas repercussões sobre usuários brasileiros no compartilhamento indevido de dados (BRASIL, 2018b). De acordo com a ementa do processo, as empresas processadas cometeram as seguintes infrações:

Infração aos direitos básicos do consumidor no que diz respeito ao reconhecimento de sua vulnerabilidade, ausência de boa-fé, ao equilíbrio entre consumidores e fornecedores, ao direito à privacidade e à intimidade. Cometimento de prática abusiva em desfavor da coletividade consumerista. Falha no dever de fornecimento de informações claras e adequadas quanto a sua política de privacidade pelas Representadas Falha na custódia adequada dos dados fornecidos pelos usuários considerando o modelo de negócios adotado (BRASIL, 2018b, p. 1).

⁷Processo nº 08012.000723/2018-19.

Portanto, de acordo com os fatos e da potencial exposição de consumidores/usuários brasileiros, houve desrespeito aos princípios básicos que regem a legislação consumerista nacional, visto que houve prática abusiva em decorrência de violação do Código de Defesa do Consumidor (CDC). Dispõe-se necessário esse artigo sobre a proteção do consumidor no que concerne o “respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo” (BRASIL, 1990, artigo 4º).

Também houve descumprimento dos artigos “4º, *caput*, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37 e art. 39” (BRASIL, 2018b, p. 1) do CDC, descumprindo os direitos básicos do consumidor e violando a publicação de publicidades enganosas e abusivas (BRASIL, 1990).

De acordo o artigo 4º, há oito princípios que atendem a Política Nacional das Relações de Consumo, os quais dizem respeito à (I) vulnerabilidade do consumidor ao consumir determinado produto e/ou serviço; (II) proteção do consumidor via ação governamental; (III) equilíbrio entre os interesses do consumidor e do fornecedor, garantindo o desenvolvimento tecnológico e econômico; (IV) informação e educação acerca dos direitos e deveres dos consumidores e fornecedores; (V) incentivo à criação de meios alternativos de soluções e conflitos de consumo, bem como de meios eficientes para o fornecimento de produtos e serviços; (VI) repressão e coibição de abusos no mercado de consumo; (VII) melhoria dos serviços públicos; (VIII) constante instrução acerca das modificações do mercado de consumo (BRASIL, 1990).

Além de infringir o CDC, houve descumprimento do Marco Civil da Internet (Lei nº 12.965/14), nos “arts. 2º, inc. II e III, e 7º, incs. VI, VII, VIII, IX, e XIII” (BRASIL, 2018b, p. 1). De acordo com o artigo 2º, “a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como [...] os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; [...]a pluralidade e a diversidade” (BRASIL, 2014, artigo 2º).

Em seu artigo 7º, o Marco Civil da Internet apresenta os direitos e as garantias dos usuários ao acessarem a internet, sendo que algumas foram descumpridas pelo *Facebook*: garantia de o usuário receber informações completas e claras ao firmar um contrato de prestação de serviço, principalmente no que fiz respeito à proteção dos dados pessoais, sendo vedado o fornecimento dos mesmos a terceiros, salvo mediante consentimento livre e esclarecido; consentimento expresso acerca da “coleta, uso, armazenamento e tratamento de dados pessoais” (BRASIL, 2014, artigo 7º); “aplicação das normas de proteção e defesa do

consumidor nas relações de consumo realizadas na internet” (BRASIL, 2014, artigo 7º, inciso XIII).

Conduto, estando caracterizada a prática de infração à legislação consumerista, nos termos da Lei Federal nº 8.078/1990, do Decreto Federal nº 2.181/1997, da Lei Federal 9.784/1999, foi determinado que os representantes sofressem uma sanção administrativa de multa, no valor de R\$ 6.600.000,00 (seis milhões e seiscentos mil reais). O recolhimento da multa aplicada foi realizado nos termos da Portaria nº 8, 5 de abril de 2017, da Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, que trata do recolhimento da multa aplicada nos processos administrativos que tramitem nessa secretaria (BRASIL, 2018b).

6 CONSIDERAÇÕES FINAIS

Levando-se em consideração o avanço da tecnologia, sendo a internet deveras utilizada atualmente, há aumento da preocupação em se garantir os direitos fundamentais da população, como a privacidade, direito de sons e imagens, proteção de dados, liberdade de expressão, inviolabilidade da intimidade, consentimento livre e esclarecido para divulgação de dados pessoais, e assim por diante.

Foi realizada pesquisa bibliográfica em trabalhos científicos e acadêmicos e pesquisa documental em documentos oficiais brasileiros, objetivando-se analisar o direito à privacidade e sua relação com a proteção de dados a partir da análise do caso concreto do *Facebook VS Cambridge Analytica*.

Para isto, os capítulos foram organizados de modo a alcançar os seguintes objetivos específicos: analisar a responsabilidade civil em atos praticados na internet; apresentar e descrever a legislação brasileira que abarcar questões relacionadas ao direito de privacidade e proteção de dados, inclusive na internet; contextualizar e analisar o caso *Facebook VS Cambridge Analytica*.

Primeiramente, pode-se observar que a proteção ao direito à privacidade se encontra regulamentada na Constituição Federal de 1988 (CF); Código de Defesa do Consumidor (CDC) (Lei nº 8.078/90); Código Civil (Lei nº 10.406/02); Marco Civil da Internet (Lei nº 12.965/14); Lei Geral de Proteção de Dados Pessoais (LGD) (Leis nº 13.709/18 e 13.853/19).

Foi possível perceber que o direito à vida privada, intimidade e imagens pessoais encontra-se regulamentado desde a Constituição Federal, sendo reafirmado pelo Código Civil de 2002 no Capítulo II, que aborda sobre os direitos de personalidade, assegurando a inviolabilidade da vida privada da pessoa natural. Os incisos X, XII, XIV do artigo 5º da

Constituição Federal atestam que todos os cidadãos possuem direito ao acesso à informação, sendo resguardado o sigilo da fonte e das comunicações telegráficas e telefônicas. Caso a intimidade, imagem pessoal, vida privada e/ou honra forem violadas, assegura-se o direito à indenização. De acordo com os artigos 17, 18 e 20 do Código Civil, salvo quando autorizado ou necessário judicialmente, não se pode utilizar o nome alheio em publicações, representações, propaganda comerciais, tampouco divulgar dados pessoais (palavras, imagens, publicações, escritos) de uma pessoa, ainda que não haja intenção difamatória.

Com relação aos direitos dos consumidores no que tange o cadastro e registro de dados pessoais, o Código de Defesa do Consumidor prevê, no inciso IV do artigo 6º, a proteção contra práticas, cláusulas e publicidade enganosa e abusiva. Sendo reconhecida a vulnerabilidade do consumidor, nos termos do artigo 4º do Código de Defesa do Consumidor, a Política Nacional das Relações de Consumo objetiva viabilizar equilíbrio nas relações entre fornecedores e consumidores, com vista à melhoria do mercado de consumo, respeito aos direitos fundamentais da pessoa humana e proteção de seus interesses econômicos.

Com o advento das tecnologias, a internet se popularizou, sendo necessário criar legislação específica para assegurar os direitos, deveres, princípios e garantias quanto ao seu uso. Portanto, no ano de 2014 foi sancionado o Marco Civil da Internet, garantindo, dentre outras coisas, a liberdade de expressão, a privacidade e a proteção dos dados pessoais, sendo vedados coleta e fornecimento de dados pessoais para terceiros sem livre consentimento do consumidor, nos termos do artigo 3º da referida lei. Sendo, atualmente, a internet essencial no direito à cidadania, de acordo com o artigo 7º do Marco Civil da Internet, é garantida a inviolabilidade da vida privada e do sigilo das informações privadas e/ou comunicadas na internet, salvo necessário por ordem judicial.

De modo a ampliar esta proteção aos dados pessoais, foi sancionada a Lei Geral de Dados Pessoais (LGPD) no ano de 2019. A partir disto, ao dispor sobre o tratamento de dados pessoais (inclusive em meios digitais), esta lei buscou proteger os direitos fundamentais de liberdade e privacidade. Portanto, conforme disposto no artigo 7º (tratamento de dados pessoais) e no artigo 11 (tratamento de dados pessoais sensíveis), o tratamento destes dados apenas poderá ser realizado mediante consentimento livre e esclarecido do titular; cumprimento de obrigações legais, administrativas e judiciais; tutela da saúde e proteção da vida de terceiros ou do próprio titular; proteção de crédito; realização de estudos por instituições de pesquisa.

Na segunda parte do trabalho foi contextualizado e analisado o caso *Facebook VS Cambridge Analytica* (C.A). Este caso ocorreu quando a C.A utilizou uma brecha no

Facebook para coletar, de forma indevida, dados pessoais de milhares de usuários, traçando seu perfil de personalidade. Estes dados foram, portanto, utilizados para promoção da campanha eleitoral de Donald Trump durante a corrida presidencial. Apesar de a maioria dos dados coletados sem consentimento dos usuários ter ocorrido nos Estados Unidos, também incidiu no Brasil.

No Brasil, o caso judicial ocorreu por meio de denúncia realizada pelo Departamento de Proteção e Defesa do Consumidor (DPCD), sendo o *Facebook* condenado, sofrendo sanção administrativa na forma de multa, no valor de seis milhões e seiscentos mil reais. Esta condenação ocorreu tendo em vista o descumprimento do Código de Defesa do Consumidor, violando os direitos básicos do consumidor; e do Marco Civil da Internet, uma vez que não houve consentimento dos usuários durante a coleta, uso e divulgação de seus dados pessoais para terceiros.

Da análise do caso em questão, em paralelo com os preceitos de nossa legislação nacional, se pode perceber que houve descumprimento dos incisos I, III e IV do artigo 4º; dos incisos II, III, IV e VI do artigo 6º, dos artigos 18, 31, 37 e 38 do Código de Defesa do Consumidor. Estes artigos asseguram as necessidades dos consumidores, seus interesses econômicos e harmonização entre os interesses do consumidor e do fornecedor (artigo 4º); os direitos básicos do consumidor, no que diz respeito à proteção contra propaganda enganosa, devendo as informações comunicadas ser claras, corretas, precisas e objetivas e ao direito à reparação de danos causados (artigo 6º e artigo 31); responsabilidade dos fornecedores sobre seus produtos e serviços (artigo 18). Ainda, o artigo 37 proíbe a publicação enganosa (falsa) e/ou abusiva, sendo capaz de induzir o consumidor ao erro; e o artigo 38 afirma que cabe ao fornecedor, patrocinador, a correção de informações e a prova de sua veracidade.

Outrossim, houve violação dos incisos II e III do artigo 2º e dos incisos VI, VII, VIII, IX e XIII do artigo 7º do Marco Civil da Internet. Conforme artigo 2º, a liberdade de expressão, a diversidade e os direitos humanos são fundamentos do uso da internet no Brasil. Conforme já especificado, o artigo 7º descreve as hipóteses em que o tratamento de dados pode ser realizado. Ao desrespeitar o direito à privacidade por não garantir o direito à proteção dos dados pessoais, o *Facebook* infringiu estes fundamentos. Para a coleta e tratamento destes dados não consentimento livre e esclarecido dos titulares, tampouco necessidade de sua utilização para cumprimento legal, judicial ou visando garantia à saúde e proteção à vida, infringindo o artigo 7º do Marco Civil da Internet.

Por conta de o processo ter ocorrido no ano de 2018, a Lei Geral de Proteção dos Dados Pessoais (LGPD) ainda não estava em vigência e, por conta disto, não foi utilizada nos

autos processuais. Se o caso fosse julgado posterior à aprovação desta lei, os fundamentos da proteção de dados teriam sido violados pelo *Facebook*.

Tendo em vista a descrição e análise da legislação nacional acerca dos direitos à privacidade e proteção de dados, dos direitos e deveres para o uso da internet, bem como de um caso em que estes direitos foram infringidos, resultando em condenação e sanção administrativa, foi possível atingir o objetivo principal deste trabalho.

Uma vez que a responsabilidade civil diz respeito à restauração de um dano causado a outrem, a fim de reparar o lesado, a mesma se aplica ao caso analisado. A sanção administrativa na forma de multa buscou reparar o dano causado aos usuários do *Facebook* que tiveram seus dados coletados e utilizados sem consentimento. Portanto, houve um agente infrator (*Facebook*); um dano ou prejuízo (invasão de privacidade e intimidade dos usuários); e um nexo de causalidade (não cumprimento dos direitos legais assegurados aos consumidores no que tange o direito à privacidade e proteção dos dados pessoais). Portanto, percebe-se que a responsabilidade civil, atualmente, encontra-se ampliada a atos ilícitos e ilegais praticados na internet.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988.

BRASIL. **Lei nº 8.078, de 11 de Setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Congresso Nacional, 1990.

BRASIL. **Lei nº 10.406, de 10 de Janeiro de 2002**. Institui o Código Civil. Brasília: Congresso Nacional, 2002.

BRASIL. **Lei nº 12.965, de 23 de Abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Congresso Nacional, 2014.

BRASIL. **Lei nº 13.709, de 14 de Agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Congresso Nacional, 2018a.

BRASIL. Ministério da Justiça e Segurança Pública. **Processo nº 08012.000723/2018-19**. Representante: Departamento de Proteção e Defesa do Consumidor – ex officio. Representados: *Facebook Inc.* e *Facebook Serviços Online do Brasil Ltda*. Brasília, 04 de Abril de 2018.

BRASIL. **Lei nº 13.853, de 8 de Julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Congresso Nacional, 2019.

CANCELIER, M. V. L. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, n. 76, 2017.

CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 240 fls. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

FARIAS, C.C.de; ROSENVALD, N.; NETTO, F.P.B. **Responsabilidade Civil**. 2º ed. São Paulo: Atlas, 2015.

FORNASIER, M. O.; BECK, C. *Cambridge Analytica*: Escândalo, Legado e Possíveis Futuros para a Democracia. **Revista Direito em Debate**, Unijuí, ano XXIX, n. 53, 2020.

GAGLIANO, P. S.; PAMPLONA FILHO, R. **Novo Curso de Direito Civil**. Volume 3: Responsabilidade Civil. 10 ed. São Paulo: Saraiva, 2012.

GARCIA, R. D. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. **Revista da Faculdade de Direito do Sul de Minas**, Pouso Alegre, v. 34, n. 1, 2018.

GONÇALVES, C. R. **Direito Civil Brasileiro**. Volume 4: Responsabilidade Civil. 12 ed. São Paulo: Saraiva, 2017.

LEONARDI, M. **Responsabilidade civil dos provedores de serviço de internet**. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, M. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

OLIVEIRA, N. A. S. História e internet: conexões possíveis. **Revista Tempo e Argumento**, Florianópolis, v. 6, n. 12, 2014.

OLIVEIRA, R. S.; BARROS, B. M. C.; PEREIRA, M. N. O direito à privacidade na Internet: desafios para a proteção da vida privada e o direito ao esquecimento. **Rev. Fac. Direito UFMG**, Belo Horizonte, n. 70, 2017.

PEIXOTO, E. L. C.; JUNIOR, M. E. O direito à privacidade na sociedade da informação. *In*: ENPEJUD, I, Maceió, 2016. **Anais...** Escola Superior da Magistratura de Alagoas, FUNDESMAL, 2016. Disponível em: <http://enpejud.tjal.jus.br/index.php/exmpteste01/issue/view/2/showToc>. Acesso em: 12 nov. 2020.

PINHEIRO, C. R. P. **Algoritmos Eleitorais**: Impacto da Mineração de Dados de uma Democracia. 2018. 40 fls. Dissertação (Mestrado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2018.

PINHEIRO, P.P. **Direito digital**. 5. ed. São Paulo: Saraiva, 2013.

PIRES, C.; NOVO, C.; GOMES, J. Navegação segura na Internet – riscos e desafios. **Revista Interações**, Santarém, Portugal, v. 6, n. 14, 2010.

PRETO, N.; PINTO, C. C. Tecnologias e novas educações. **Revista Brasileira de Educação**, Rio de Janeiro, v. 11, n. 31, 2006.

PRIMI, R. Avaliação Psicológica no Século XXI: de Onde Viemos e para Onde Vamos. **Psicol. cienc. prof.**, Brasília, v. 38, n. especial, 2018.

SERRA, N. C. **Proteção de dados pessoais e Facebook**: análise sobre privacidade de dados na internet. 2018. 112 fls. Monografia (Graduação em Direito) – Universidade de Brasília, Brasília, 2018.

SILVA, J. A. da. **Curso de Direito Constitucional Positivo**. 43 ed. São Paulo: Malheiros, 2020.

VENOSA, S.S. **Direito civil**. Direitos e Responsabilidade Civil. 19. ed. São Paulo: Atlas, 2019.

VIEIRA, T. M. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 fls. Dissertação (Mestrado em Direito, Estado e Sociedade: Políticas Públicas e Democracia) – Universidade de Brasília, Brasília, 2007.

WENDT JÚNIOR, A.; EHRHARDT, F. F.; SILVA, R. L. da. Sociedade em rede: caso *Cambridge Analytica* e a Lei nº 13.709/2018 uma análise do seu potencial de proteção aos dados dos usuários. *In*: Congresso Internacional de Direito e Contemporaneidade, 5, Santa Maria, 2019. **Anais...** Santa Maria, 2019.

CURSO DE BACHARELADO EM DIREITO**TERMO DE AUTENTICIDADE DO ARTIGO**

Eu, Amanda Thaís Bonette, acadêmico/a regularmente matriculado/a na disciplina de Trabalho de Curso (TC) II declaro que o artigo apresentado foi escrito por mim e que não há cópia de obras impressas ou eletrônicas de nenhum tipo.

Ponta Grossa, 25 de Novembro de 2020.