

A CAMBRIDGE ANALYTICA, O MARCO CIVIL DA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS

CAMBRIDGE ANALYTICS, THE INTERNET CIVIL FRAMEWORK AND THE GENERAL DATA PROTECTION LAW

Recebido: 22/05/2024

Aceito para publicação: 29/05/2024

Marcelo Bueno Espanha

Mestre em Políticas Públicas pela Universidade de Mogi das Cruzes
Instituição: Centro Universitário ETEP (ETEP)

Endereço: Avenida Barão do Rio Branco, 882 - Jardim Esplanada, São José dos Campos - SP,
12242-800

E-mail: marcelo.espanha@etep.edu.br

ORCID: <https://orcid.org/0009-0003-6630-4410>

João Marcelo Domingos Sousa

Graduando do Curso de Direito pelo Centro Universitário ETEP
Instituição: Centro Universitário ETEP (ETEP)

Endereço: Avenida Barão do Rio Branco, 882 - Jardim Esplanada, São José dos Campos - SP,
12242-800

E-mail: Sousabuy@gmail.com

ORCID: <https://orcid.org/0009-0000-1629-4339>

Sarah Maria Gonzaga Da Silva

Graduanda do Curso de Direito pelo Centro Universitário ETEP
Instituição: Centro Universitário ETEP (ETEP)

Endereço: Avenida Barão do Rio Branco, 882 - Jardim Esplanada, São José dos Campos - SP,
12242-800

E-mail: sarah05maria11@gmail.com

ORCID: <https://orcid.org/0009-0002-6664-4602>

Lucas Felipe Santos Veloso

Graduando do Curso de Direito pelo Centro Universitário ETEP
Instituição: Centro Universitário ETEP (ETEP)

Endereço: Avenida Barão do Rio Branco, 882 - Jardim Esplanada, São José dos Campos - SP,
12242-800

E-mail: web.lukasoft@gmail.com

ORCID: <https://orcid.org/0009-0000-5336-4535>

Rafael Eduardo De Paula Pereira

Graduando do Curso de Direito pelo Centro Universitário ETEP
Instituição: Centro Universitário ETEP (ETEP)

Endereço: Avenida Barão do Rio Branco, 882 - Jardim Esplanada, São José dos Campos - SP,
12242-800

E-mail: rafaeduardo2010@hotmail.com

ORCID: <https://orcid.org/0009-0003-2289-2361>

RESUMO

Este ensaio acadêmico analisa hipoteticamente o caso *Cambridge Analytica* à luz do Direito Digital brasileiro e seu impacto na sociedade. A *Cambridge Analytica* foi uma empresa inglesa que coletava dados irregularmente nas redes sociais (por exemplo, *Facebook*) utilizando algoritmos, para violar a privacidade dos usuários, assim como para influenciar as eleições americanas e o plebiscito do *Brexit*, além de espalhar notícias falsas. A proteção de dados é um direito fundamental previsto no art. 5º, inciso LXXIX da Constituição Federal. Na esfera infraconstitucional, temos a Lei nº 12.965/2012 (Marco Civil da *Internet*) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), são instrumentos do Direito Digital brasileiro que está surgindo. O objetivo do presente ensaio é descrever escândalo *Cambridge Analytica*, os diplomas jurídicos do Direito Digital brasileiro e refletir sobre sua aplicação se o caso *Cambridge Analytica* ocorresse no Brasil. A metodologia utilizada foi a revisão narrativa da literatura e da legislação.

Palavras-chave: *Cambridge Analytica*, Marco Civil da *Internet*, LGPD, violação de dados, privacidade, Direito Digital.

ABSTRACT

This academic essay hypothetically analyzes the *Cambridge Analytica* case in light of Brazilian Digital Law and its impact on society. *Cambridge Analytica* was an English company that irregularly collected data on social networks (for example, *Facebook*) using algorithms to violate users' privacy, as well as to influence the American elections and the *Brexit* plebiscite, in addition to spreading fake news. Data protection is a fundamental right provided for in art. 5th, item LXXIX of the Federal Constitution. In the infraconstitutional sphere, we have Law No. 12,965/2012 (Marco Civil da *Internet*) and Law No. 13,709/2018 (General Data Protection Law – LGPD), which are instruments of Brazilian Digital Law that are emerging. The objective of this essay is to describe the *Cambridge Analytica* scandal, the legal diplomas of Brazilian Digital Law and reflect on their application if the *Cambridge Analytica* case occurred in Brazil. The methodology used was a narrative review of literature and legislation.

Keywords: *Cambridge Analytica*, Marco Civil da *Internet*, LGPD, data breach, privacy, Digital Law.

1. INTRODUÇÃO

O presente ensaio acadêmico busca estudar o caso *Cambridge Analytica*, que ocorreu no exterior, à luz do Direito Digital Brasileiro, para aferir hipoteticamente como a legislação brasileira trataria do caso.

A *Cambridge Analytica* foi uma empresa subsidiária do *SCL Group*, que minerava e tratava dados nas redes sociais de forma ilícita, interferindo em eleições e propagando *Fake News* (Fornasier, Beck, 2020).

Ensaio 1

O Direito Digital no Brasil é recente, sendo que o nosso ordenamento jurídico possui poucas normas jurídicas sobre o tema.

Inicialmente destacamos o art. 5º, LXXIX da Constituição Federal, por esse dispositivo constitucional temos que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 1988). Ressalta-se que a inclusão de dados na Constituição Federal¹ ocorreu em 2022 pela Emenda Constitucional nº 115/2022 (Brasil, 1988). Com efeito, o inciso LXXIX do art. 5º da Constituição Federal faz parte do Direito Digital do Brasil.

A segunda lei que compõe o Direito Digital em nosso país é a Lei nº 12.737/2012, conhecida por Lei a Carolina Dickmann, que estabeleceu os crimes informáticos alterando dispositivos do Código Penal (Brasil, 2012). Sem dúvida essa legislação faz parte do Direito Digital brasileiro, porém como o viés do presente ensaio é a proteção de dados e não crimes digitais, não a analisaremos na sequência do estudo.

A terceira lei que forma o arcabouço legislativo do Direito Digital brasileiro é Lei nº 12.965/2014. O Marco Civil da *Internet* estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e determina as diretrizes para atuação da União, Estados, Distrito Federal e Municípios (Brasil, 2014).

A quarta lei que compõe o Direito Digital Brasileiro é a Lei nº 13.709/2018, Lei de Geral de Proteção de Dados (LGPD), ela dispõe “sobre o tratamento de dados pessoais a fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018).

Além dessas normas de Direito Digital supramencionadas, utilizaremos o Código Civil e as normas sobre responsabilidade civil para o nosso estudo.

A metodologia do presente ensaio, é a revisão narrativa da literatura e da legislação. O objetivo do trabalho é estudar hipoteticamente o *caso Cambridge Analytica* com base na legislação brasileira.

O tema é relevante, pois “relatórios de 2018 da *We Are Social* e da *Hootsuite* afirmam que os brasileiros passam, em média, mais de nove horas diárias navegando na Internet (Kemp, 2018, *apud* Caldas e Caldas, 2019). Segundo dados do *Facebook*, cento

¹ A Constituição Federal é a lei mais importante do Brasil, ela define quem exerce o poder, como o poder é exercido, qual a relação entre quem exerce o poder e as pessoas. E mais importante: é a Constituição o fundamento de validade para toda a legislação brasileira.

Ensaio 1

e dois milhões de brasileiros “compartilham seus momentos no *Facebook* todos os meses” (Facebook, 2016, *apud* Caldas e Caldas, 2019), logo casos como o *Cambridge Analytica* poderiam impactar a sociedade brasileira.

2. CAMBRIDGE ANALYTICA

“Nesta segunda década do século XXI, as tecnologias digitais tornaram-se ainda mais ubíquas – especialmente com a notável expansão da *Internet* móvel” Caldas e Caldas, 2019). E neste contexto temos as figuras das *big datas*.

De acordo com Saldanha *et. al.* (2021):

“(...) big data é um dos aspectos do campo da ciência de dados que trata de outros aspectos, como estratégias para extração, transformação e carga dos dados, modelagem, construção e avaliação de algoritmos descritivos e preditivos, visualização de grandes quantidades de dados e deploy dos modelos em ambientes de produção para a tomada de decisão, entre outros.

O que importa na definição de big data não é o volume ou mesmo a velocidade da produção de dados, mas a complexidade estrutural desses dados (variedade) e o poder computacional necessário para analisá-los integralmente. (...)”

E o caso Cambridge Analytica é um exemplo de como a *big data* pode ter influência influenciar a vida das pessoas.

A empresa *Cambridge Analytica*, esteve por trás de campanhas como a do Brexit, no Reino Unido, e do ex-presidente dos Estados Unidos, Donald Trump (Caldas e Caldas, 2019). Era uma pessoa jurídica de direito privado, de origem inglesa, que esteve sob os holofotes nos últimos meses às custas de um escândalo envolvendo a corporação Facebook e dados pessoais de milhões de usuários (Caldas e Caldas, 2019).

Em 2015, Harry Davies² revelou que a empresa coletou dados do *Facebook* para a campanha presidencial estadunidense de 2016 do senador Ted Cruz. Investigações expuseram a influência nos votos do *Brexit* pela saída do Reino Unido da União Europeia (Fornasier e Beck, 2020).

Christopher Wylie foi o primeiro a denunciar a *Cambridge Analytica* com provas e dados confidenciais. Brittany Kaiser, ex-funcionária, expôs mais coletas ilícitas de dados via teste de personalidade no *Facebook*. A CA usou IA e *machine learning* para segmentar e polarizar grupos sociais (Fornasier e Beck, 2020).

Segundo Fornasier e Beck (2020) o *modus operandi* da *Cambridge Analytica*

² Jornalista do *The Guardian* que fez a primeira denúncia contra a *Cambridge Analítica*. (FORNASIER e BECK, 2020)

Ensaio 1

envolvia três passos:

“O primeiro responsável pela coleta, armazenamento e tratamento de dados pessoais no *Facebook*, incluindo, a título meramente exemplificativo, fotos pessoais, posts insignificantes do cotidiano, lista de amigos, lista de pessoas bloqueadas, grupos que as pessoas ingressaram e grupos que participam ativamente (...)

O segundo grupo era responsável – no curso das eleições americanas de 2016 – por uma tarefa mais complexa. Funcionários Sênior da empresa – como é o caso de Brittany Kaiser – tinham de minerar as informações (*data mining*) desse enorme banco de dados e, por este processo, buscar em Estados da Confederação Americana os votos indecisos (votos que poderiam ir tanto para o lado Conservador quanto para o lado Democrata) (...)

O último grupo de funcionários da *Cambridge Analítica* funcionava de forma quase clandestina a tudo que é ético, democrático e contrário ao espírito dos *Founding Fathers* (fundadores do Estados Unidos da América). Trata-se, em síntese, de traição a todo um processo democrático que deve sempre ser vigiado e tutelado. Este último grupo, em que muitos funcionários da empresa até hoje alegam que desconheciam as práticas descritas a seguir, tornou-se uma ferramenta maliciosa extremamente eficiente (...).”

Em 2018 a *Cambridge Analytica* teve falência decretada, e todos os arquivos da empresa permaneceram sob investigação e sigilo judicial (Fornasier e Becker, 2020). Ressalta-se que a *Cambridge Analytica* tinha uma parceria com a empresa brasileira CA-Ponte (Fornasier e Becker, 2020), o que reforça a importância de analisar a *Cambridge Analytica* à luz da legislação brasileira.

3. ARTIGO 5º, LXXIX DA CONSTITUIÇÃO FEDERAL

Os direitos fundamentais surgem com a queda do Estado Absolutista, com o surgimento do Estado constitucional, cuja essência reside na proteção dos direitos fundamentais do homem (Sarlet, 2012, p. 24, *apud* Scheuermann, 2023).

O art. 5º da Constituição Federal, veicula direitos fundamentais (Brasil, 1988). Todos os direitos materializados no art. 5º da Carta Magna, são cláusulas pétreas nos termos do art. 60, §4º, IV da Constituição (Brasil, 1988).

O Constituinte de 1988 já protegia a privacidade das pessoas. No artigo 5º, inciso X da Constituição Federal, temos que “são invioláveis a intimidade, a vida privada, a

Ensaio 1

honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1998).

Desde a promulgação da Constituição Federal em 5 de outubro de 1988 (Brasil, 1988), o mundo passou por várias transformações. As relações humanas têm migrado do espaço físico para os digitais, nossas informações estão disponíveis na *Internet*, nas redes sociais, como *Facebook*, *Twitter* e *Instagram* (Scheuermann, 2023).

A inserção de dados pessoais no ciberespaço, fragiliza e torna vulneráveis a privacidade e a intimidade dos usuários (Scheuermann, 2023), *vide* o escândalo da *Cambridge Analytica*.

A Emenda Constitucional nº 115/2022 que inseriu o inciso LIXXIX no art. 5º da Constituição Federal foi oriunda da preocupação com o escândalo da *Cambridge Analytica* segundo Scheuermann (2023). De acordo com o art. 5º, LXXIX da Constituição Federal, “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 1988).

Constitucionalizar a proteção de dados é um marco no Direito Digital do Brasil, pois a Constituição é fundamento de validade para as demais normas do ordenamento jurídico brasileiro e um vetor de interpretação do Direito.

4. MARCO CIVIL DA INTERNET

De acordo com art. 5º, I, da Lei nº 12.965/14 a *internet* constitui-se no conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados por meios de diferentes redes (Brasil, 2014). O Marco Civil da *Internet*, em seus artigos 18 e seguintes, trata da responsabilidade por danos decorrentes de conteúdo gerados por terceiros (Brasil, 2014).

Conforme Maria Helena Diniz (Diniz, 2010, p. 50) a responsabilidade civil é:

“é a aplicação de medidas que obriguem alguém a reparar o dano moral ou patrimonial causado a terceiros em razão de ato do próprio imputado, de pessoa por quem ele responde, ou de fato, de coisa ou de animal sob sua guarda, ou, ainda, de simples imposição legal.”

Com efeito, o art. 927 do Código Civil determina que aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. De acordo com o art.

Ensaio 1

186 do Código Civil a ação ou omissão voluntária, negligência ou imprudência que violar direito e causar dano a outrem, ainda que exclusivamente moral, é ato ilícito (Brasil, 2002). O ato ilícito também se configura no caso do abuso do direito, nos termos do art. 187 do código civil (Brasil, 2002). Destacando que a internet não é “terra de ninguém”, qualquer pessoa que cometa ato ilícito deverá ser responsabilizada. O Marco Civil da *Internet* contém fundamentos para esta responsabilização.

De Jesus & Milagre (2014), afirmam que o Marco Civil é:

a primeira lei infraconstitucional que regulamenta sobre a indenização por dano moral ou material por conta de violações a intimidade e vida privada no âmbito da internet. Nesse sentido o art. 7, ins. I, o MCI, traz a possibilidade da indenização por danos morais ou materiais, decorrente da violação a privacidade.

Em relação ao art. 3º da Lei n. 12.965/2014 (Brasil, 2014) temos princípios que norteiam o uso da *internet*: a) garantia da liberdade de expressão; b) proteção da privacidade; c) Proteção dos dados pessoais, na forma da lei.

O Marco Civil da *Internet* traz os direitos e garantias dos usuários em relação à proteção de Dados. Os usuários da *internet* têm direito à: inviolabilidade da intimidade; ao sigilo do fluxo de suas comunicações; a quebra do sigilo mediante a ordem judicial; ao não fornecimento de dados a terceiros; a informações claras sobre o armazenamento dos dados pessoais; ao consentimento expresso para coleta de dados; a exclusão definitiva de dados pessoais (Brasil, 2014).³

No regime jurídico o provedor não será responsabilizado por danos ocasionados por conteúdo gerado por terceiros, nos termos do artigo 18 (Brasil, 2014). A responsabilidade do provedor consubstancia-se quando não é retirado da *internet* conteúdo lesivo, conforme art. 21 da Lei nº 12.965/2014 (Brasil, 2014). No julgamento do Recurso Extraordinário 1.037.396, o Supremo Tribunal Federal, fixou o Tema 0987, sobre a responsabilidade do provedor (STF, 2018). De acordo com o art. 19 da Lei n. 12.965/2014 (Marco Civil da *Internet*), a responsabilidade do provedor é a do judicial *notice end take down*⁴.

³ Art. 7º, I, II, III e VII, VIII, IX, X da Lei nº 12965/2014 (Brasil, 2014).

⁴ *Judicial notice end take down* nada mais é do que a obrigação do provedor retirar o conteúdo ilícito da *internet* apenas depois da ordem judicial. Como exceção o art. 21 do Marco Civil da *Internet* estabelece o

Ensaio 1

Nesse regime, a responsabilidade do provedor ocorre somente se ele não retirar o conteúdo ilícito depois da ordem judicial.⁵

“A coleta de informações e dados e informações pessoais surge na chamada Web 3.0” (Loth *et al.*, 2019, *apud* Scheuermann, 2023), “que consegue gerenciar uma quantidade imensa de dados e, inclusive, determinar perfis dos usuários por meio de algoritmo” (Scheuermann, 2023).

Em relação à proteção de dados o Marco Civil, “em seu art. 7º, inciso VII criou o chamado *opt-in*, que é a necessidade de consentimento de forma expressa do usuário quanto ao uso de seus dados pessoais (Barreto Junior; Sampaio; Gallinardo, 2018, *apud* Scheuermann, 2023).

Os arts. 10 a 17 da Lei nº12.965/2014 tratam da proteção de dados (Brasil, 2014), vejamos os pontos mais importantes desses dispositivos do Marco Civil da *Internet*.

Pelo art. 10, a guarda e disponibilização dos registros de conexão e de acesso à *internet*, bem como de dados pessoais e do conteúdo de comunicações privadas, devem preservar a intimidade, a vida privada, a honra e imagem (Brasil, 2014).

No *caput* do art. 11 do Marco Civil, temos importante norma sobre a lei no espaço (Brasil, 2014):

“ (...) Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.()”

Além da possibilidade de aplicação da lei brasileira no caso de violações de registros, dados e comunicações, nos termos do art. 12 do Marco Civil da Internet, aplicam-se sanções civis, penais e administrativas (Brasil, 2014). O próprio art. 12 estabelece sanções administrativas: advertência, multa, suspensão temporária das atividades e proibição de exercício das atividades (Brasil, 2014).

Os arts. 13 a 17 do Marco Civil da Internet tratam da responsabilidade de guarda

notice end take down, ou seja, o provedor seria obrigado a retirar o conteúdo ilícito da *internet*, em casos de nudez ou atos sexuais privados, mediante simples notificação do interessado.

⁵ Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Ensaio 1

de registros de acesso, a cargo dos provedores, a fim de proteger a privacidade dos usuários (Brasil, 2014).⁶⁷⁸⁹

Diante do exposto, é possível verificar que o Marco Civil da *Internet* possui normas jurídicas que disciplinam o conteúdo veiculado na *internet*, bem como, a responsabilidade do provedor em relação à proteção de registros, dados e comunicação.

Há algumas normas sobre a responsabilidade do provedor na coleta, armazenamento e tratamento de dados, porém sem tratar de forma abrangente a proteção de dados, por isso o surgimento da Lei Geral de Proteção de Dados para disciplinar de maneira mais efetiva o tema e complementar o arcabouço jurídico do Direito Digital brasileiro.

5. LEI GERAL DA PROTEÇÃO DE DADOS - LGPD

Scheuermann (2023) aponta que “ciberespaço das redes sociais, criou-se uma espécie de costume em aceitar os termos de uso das aplicações sem ter ideia do que está contido em seu interior”. E essas permissões de uso com válvulas de escape foi isso que permitiu à *Cambridge Analytica* operar.

Vejamos o termo de uso do Facebook de 2022 que veicula brechas na coleta, armazenamento e compartilhamento de dados com terceiros (*Facebook*, 2022, *apud* Scheuermann, 2023):

“(...) Especificamente, quando você compartilha, publica ou carrega conteúdo protegido por direitos de propriedade intelectual nos nossos Produtos ou a eles relacionados, você nos concede uma licença não exclusiva, transferível, sublicenciável, isenta de royalties e válida mundialmente para hospedar, usar, distribuir, modificar, veicular, copiar, reproduzir publicamente ou exibir e traduzir seu conteúdo, assim como criar trabalhos derivados dele, (de modo consistente com as suas configurações de privacidade e do aplicativo). Isso significa, por exemplo, que se você compartilhar uma foto no Facebook, você nos dará

⁶ Art. 13. Na provisão de conexão à *internet*, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

⁷ Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de *internet*.

⁸ Art. 15. O provedor de aplicações de *internet* constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de *internet*, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

⁹ Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de *internet* não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Ensaio 1

permissão para armazená-la, copiá-la e compartilhá-la com outras pessoas (reforçando, de modo consistente com suas configurações), como os Produtos da Meta ou provedores de serviços que fornecem suporte para esses produtos e serviços. Vale destacar que, quando excluimos seu conteúdo dos nossos sistemas, essa licença é encerrada. (...)”

Após o escândalo de dados pessoais comercializados para fins políticos pela Cambridge Analytica, o Brasil avançou na legislação e aprovou a Lei Geral de Proteção de Dados, Lei nº 13. 709/2018 (Scheuermann, 2023). Sobre a origem da Lei Geral de Proteção de Dados, segundo Almeida e Soares (2022): ela entrou em vigor no Brasil, em 14 de agosto de 2018, tendo por inspiração o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* - GDPR)¹⁰.

De acordo com o art. 1º da Lei Geral de Proteção de Dados, ela dispõe sobre o tratamento de dados pessoais, por meios digitais, por pessoa natural ou jurídica de Direito Público ou Privado, para proteger a liberdade, a privacidade e o desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

A LGPD é uma norma com características extraterritoriais, de interesse nacional, que deve ser observada pela União, Estados, Distrito Federal e Municípios (Junior, 2019, p.4). Não é uma lei exclusiva para o sistema financeiro e visa dar uma aplicação mais prática e uniforme às leis de privacidade de dados, confidencialidade e de segurança da informação (Junior, 2019, p.4). Ainda, visa perfectibilizar os princípios e direitos fundamentais da pessoa humana, tais como o direito à intimidade, à vida privada, à honra, à imagem e ao sigilo de informações sensíveis ou de caráter personalíssimo (Junior, 2019, p.4).

O art. 65 da LGPD dispõe sobre a *vacatio legis*.¹¹ A primeira *vacatio legis* foi em 24 meses após a data de sua publicação. O segundo prazo foi incluído pela Lei nº 13.853, de 2019, mostrando a complexidade para as empresas se adequarem as exigências da norma (Brasil, 2018).

As sanções da LGPD estão incluídas no seu art. 52, ou seja, advertência, multa, suspensão, e proibição parcial ou total das atividades relacionadas ao tratamento de dados (Brasil, 2018). Para fiscalizar o cumprimento da LGPD, foi criada a Autoridade

¹⁰ sigla em inglês da União Europeia.

¹¹ Vacatio Legis é o período entre a publicação da lei e a sua vigência. Este período é necessário para a adaptação às novas diretrizes da legislação.

Ensaio 1

Nacional de Proteção de Dados (ANPD). A primeira autuação da ANPD foi para empresa *Telekall InforService*, totalizando o valor de R\$ 14.400 em multa conforme o Processo Administrativo Sancionador nº 00261.000489/2022-62 (ANPD, 2023).

Em uma pesquisa realizada pelo site LGPD Brasil, aponta que apenas 36% das empresas brasileiras estão em conformidade total com a referida lei (LGPD Brasil, 2020). Os principais obstáculos para se adequarem alegam dificuldade no mapeamento de processos, treinamento de colaboradores, segurança dos dados entre outras medidas (LGPD Brasil, 2020).

6. CAMBRIDGE ANALYTICA À LUZ DO MARCO CIVIL DA INTERNET E DA LGPD

O escândalo do Cambridge Analítica foi um exemplo de mineração de dados pessoais de usuários das redes sociais para influenciar em campanhas políticas. Se a Cambridge Analítica atuasse no Brasil, o Marco Civil da *Internet* e a Lei Geral de Proteção de Dados teriam incidência?

Embora o Marco Civil da *Internet* em seu art. 3º garantir a proteção de dados dos usuários na *internet*, não há menção às redes sociais, somente aos provedores de *internet* (Brasil, 2014). Diante disso, o Marco Civil da *Internet* teria aplicação parcial se a *Cambridge Analytica* atuasse no Brasil, haja vista seu foco ser os provedores.

Em relação a LGPD, logo no seu art. 1º, o legislador deixou claro o objetivo era proteger os dados (inclusive digitais), a fim de proteger direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade (Brasil, 2018). No seu art. 6º, incisos I à X, temos inúmeros princípios que protegem a coleta, o tratamento e a destinação dos dados pessoais, a fim de que a boa-fé prevaleça (Brasil, 2018).

Neste contexto, nos parece que se a *Cambridge Analytica* operasse no Brasil, a LGPD seria o principal instrumento jurídico para proteger os usuários das redes sociais. Ademais, é nítido que a mineração de dados e uso político pelas *Big Datas* fere não só os princípios da LGPD, mas também inúmeras regras, por exemplo: A *Cambridge Analytica* obteve sem consentimento grande volume de informações pessoais de usuários do *Facebook* (Fornasier, Back, 2020), o que fere a regra do art. 7º da LGPD que exige consentimento do titular do dado.

7. CONCLUSÃO

A análise da violação de dados no caso *Cambridge Analytica* revela profundas implicações para a sociedade, especialmente quando considerada sob a ótica da proteção à privacidade, bem como à luz do Direito Digital. A *Cambridge Analytica*, envolveu-se em práticas ilícitas de mineração e tratamento de dados nas redes sociais, interferindo em eleições e propagando notícias falsas (Fornasier, Beck, 2020). Este caso evidenciou a fragilidade dos sistemas de proteção de dados e a vulnerabilidade dos direitos individuais na era digital.

No Brasil, o Direito Digital é recente, basicamente temos o art. 5º, LXXIX, da Lei nº 12.965/2014 (Marco Civil da *Internet*) e pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). O Marco Civil da *Internet* estabelece princípios e diretrizes para o uso da *internet*, assegurando direitos e deveres tanto para usuários quanto para provedores de serviços. A LGPD, por sua vez, dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O caso *Cambridge Analytica* serve como um alerta para a importância do aprimoramento da regulamentação e da aplicação do Direito Digital no Brasil, para que a proteção dos usuários seja mais efetiva.

REFERÊNCIAS

ALMEIDA, S. do C. D. de; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26–45, jul. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261000489_2022_62_decisao_telekall_inforsevice.pdf. Acesso em: 10 maio 2024.

BRASIL. **Constituição Federal de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 maio 2024.

BRASIL. **Lei nº 10.406/2002, Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 19 abril 2024.

Ensaio 1

BRASIL. **Lei nº 12.737/2012 (Lei a Carolina Dickmann)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 de maio de 2024.

BRASIL. **Lei nº 12.965/2014, Marco Civil da Internet**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 abr. 2024.

BRASIL. **Lei nº 13.709/2018, Lei Geral de Proteção de Dados**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 abr. 2024.

CALDAS, Camilo Onoda Luiz; CALDAS, Pedro Neris 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**, v.24, n.2, p.196-220, abr./jun. 2019. Disponível em: <https://www.scielo.br/j/pci/a/4qKvdJBT8svQshQdhfrz8jN/#>. Acesso em: 05 de abril 2024

CARVALHO, Patrícia Heloisa de. **Revista da Faculdade de Direito do Sul de Minas**, Pouso Alegre.

DE JESUS, Damásio; MILAGRE, José Antonio. **Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo: Saraiva, 2014.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. 24. ed., v. 7. São Paulo: Saraiva, 2010.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia. **Revista Direito em Debate**, 2020, v. 29, nº 53, p. 182-195. Disponível em: <http://dx.doi.org/10.21527/2176-6622.2020.53.182-195>. Acesso em: 22 mar. 2024.

JUNIOR, Mauricio Armomino de. **Manual de Implementação da Lei Geral de Proteção de Dados**. 1. ed. v. 1. São Paulo: Via Ética, 2019.

LGPD Brasil. Disponível em: <https://www.lgpdbrasil.com.br/aderencia-a-lgpd- apenas-36-das-empresas-brasileiras-estao-em-conformidade-total/#:~:text=Paralelamente%20a%20essa%20tend%C3%Aancia%2C%20houve,ano%2C%20atingindo%20apenas%206%25>. Acesso em: 10 maio 2024.

SALDANHA, Raphael de Freitas, BARCELLOS, Christovam; PEDROSO, Marcel de Moraes. Ciência de dados e big data: o que isso significa para estudos populacionais e da saúde? **Caderno Saúde Coletiva [Internet]**. 2021;29(setembro), p.51–58. Disponível em: <https://doi.org/10.1590/1414-462X202199010305>. Acesso em: 10 de abril de 2024.

Ensaio 1

SCHEUERMANN. Gabriela Felden. DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL AUTÔNOMO A PARTIR DA EMENDA CONSTITUCIONAL Nº 11512022. **Revista da Defensoria Pública RS**. Porto Alegre, ano 14, volume 2, n. 33, p. 253-274, 2023. Disponível em: <https://orcid.org/0000-0003-0839-8335>. Acesso em: 24 de maio de 2024.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário 1.037.396, Tema 0987, 2018**. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=987>. Acesso em: 19 abr. 2024.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. **Marco Civil da Internet, 2016**. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/educacao-semanal/marco-civil-da-internet>. Acesso em: 03 maio 2024.