UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
BACHARELADO EM DIREITO

JOÃO LUCAS FERNANDES DA COSTA LOPES

A LEI Nº 13.709/2018 E A EFICÁCIA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL FRENTE À GENERAL DATA PROTECTION REGULATION, À LUZ DO CASO CAMBRIDGE ANALYTICA

FORTALEZA
2022

JOÃO LUCAS FERNANDES DA COSTA LOPES

A LEI Nº 13.709/2018 E A EFICÁCIA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL FRENTE À GENERAL DATA PROTECTION REGULATION, À LUZ DO CASO CAMBRIDGE ANALYTICA

Monografia apresentada ao curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Profa. Fernanda Cláudia Araújo da Silva, Msc.

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L853l Lopes, João Lucas Fernandes da Costa.
A Lei n° 13.709/2018 e a eficácia na proteção de dados pessoais no Brasil frente à General Data Protection Regulation, à luz do caso Cambridge Analytica / João Lucas Fernandes da Costa Lopes. – 2022.
40 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2022.
Orientação: Profa. Ma. Fernanda Cláudia Araújo da Silva.

1. Proteção de dados. 2. Privacidade. 3. Lei Geral de Proteção de Dados. 4. Direito Europeu. 5. Cambridge Analytica. I. Título.

CDD 340

JOÃO LUCAS FERNANDES DA COSTA LOPES

A LEI Nº 13.709/2018 E A EFICÁCIA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL FRENTE À GENERAL DATA PROTECTION REGULATION, À LUZ DO CASO CAMBRIDGE ANALYTICA

Monografia apresentada ao curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____
Profa. Fernanda Cláudia Araújo da Silva (Orientadora)
Universidade Federal do Ceará (UFC)

_____
Antonio Alex Dayson Tomaz
Universidade Federal do Ceará (UFC)

_____
Josélia da Silveira Nogueira
Universidade Federal de Santa Catarina (UFSC)

RESUMO

A proteção de dados se mostra como uma das principais discussões acerca do Direito à Privacidade no âmbito digital, em especial na relação dos cidadãos com as redes sociais. O presente trabalho tem como escopo realizar uma análise comparativa entre a Lei Geral de Proteção de Dados (LGPD) e a General Data Protection Regulation (GDPR), identificando os mecanismos jurídicos que foram preservados na legislação brasileira a partir do direito europeu, à luz do caso Cambridge Analytica. Para tanto, busca-se compreender a origem da proteção de dados e o processo de construção dos conceitos sob influência do direito europeu até os dias atuais, passando pela consolidação legislativa na União Europeia até culminar na entrada em vigor da LGPD. O objetivo é identificar como a LGPD incorpora os principais conceitos da proteção de dados a partir da evolução jurídica até os dias atuais, bem como analisar a contribuição do caso Cambridge Analytica na consolidação dessas leis e avaliar em que medida a lei brasileira é capaz de garantir a eficácia da proteção de dados frente a casos complexos como o da Cambridge Analytica.

Palavras-chave: Proteção de Dados. Privacidade. Lei Geral de Proteção de Dados. Direito Europeu. Cambridge Analytica.

ABSTRACT

Data protection is one of the main discussions about the Right to Privacy in the digital sphere, especially in the relationship between citizens and social networks. The scope of this paper is to carry out a comparative analysis between the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR), identifying the legal mechanisms that were preserved in Brazilian legislation from European law, in the light of the Cambridge Analytica case. To this end, it aims to understand the origin of data protection and the construction process of concepts under the influence of European law until the present day, through the legislative consolidation in the European Union until culminating in the entry into force of the LGPD. The objective is to identify how the LGPD incorporates the main concepts of data protection from the legal evolution to the present day, as well as to analyze the contribution of the Cambridge Analytica case in the consolidation of these laws and to evaluate to what extent the Brazilian law can guarantee the effectiveness of data protection in complex cases such as Cambridge Analytica.

Keywords: Data Protection. Privacy. General Data Protection Law. European Law. Cambridge Analytica.

SUMÁRIO

1 INTRODUÇÃO

A transformação tecnológica é uma dádiva trazida pelo século XXI que transformou a convivência em sociedade. A possibilidade de comunicação em tempo real por diversos canais, o compartilhamento de informações cotidianas e a digitalização de nossa vida privada são características que passaram a nos acompanhar desde então, e que cada vez mais tornam-se indispensáveis.

Não obstante, o Direito, como instrumento que rege as interações na sociedade civil, também seria afetado por tal transformação. Não apenas a criação de novos meios de interação, mas a exponencialidade do avanço tecnológico trouxe a necessidade de mecanismos jurídicos que fossem capazes de capturar a essência dessa mudança, ao passo em que pudessem permanecer atuais em tempos de transformação constante.

A proteção de dados pessoais tem adquirido uma posição central dentro da necessidade de adaptação legislativa. A alta capacidade de processamento de dados fez com que estes se tornassem um valioso ativo mercadológico, razão pela qual plataformas e intermediários buscam capturar a atenção de seus usuários a fim de engajá-los. As leis observam tais relações e tentam equilibrar o relacionamento entre provedores e tomadores, para que os benefícios da integração possam ser usufruídos dentro da preservação dos direitos fundamentais.

O movimento de adaptação inicia-se na Europa e rapidamente espalha-se para outros territórios, incluindo o Brasil. Apesar de veloz e efetivo, alguns acontecimentos foram cruciais para modelagem do cenário jurídico que encontramos atualmente, e cabe uma análise sobre como os mecanismos jurídicos atuais, especialmente o brasileiro – representado pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados – se tornaram capazes não apenas de antever determinados conflitos decorrentes do uso indevido de dados pessoais, mas especialmente coibi-los.

Dentre esses eventos, o presente trabalho destaca a crise global gerada pela utilização indevida de dados advindos do Facebook por parte da consultoria

política Cambridge Analytica, com o fito de trazê-la como ponto focal de uma análise comparativa entre a Lei Geral de Proteção de Dados e a *General Data Protection Regulation*, da União Europeia. A ocasião, por sua gravidade, acelerou as discussões legislativas ao redor do mundo para garantir uma proteção efetiva aos usuários, bem como segurança jurídica às organizações que, por vontade ou necessidade, trabalhassem no processamento de dados pessoais.

A metodologia utilizada envolveu pesquisas bibliográficas e consulta a principais relatos jornalísticos da ocasião para descrição e detalhamento dos fatos, com o objetivo de, além de ilustrar a problemática, estabelecer a relevância da situação dentro do contexto jurídico atual e como ainda se relaciona com as legislações em vigor.

No primeiro capítulo, será abordada uma perspectiva geral sobre o Direito à Proteção de Dados Pessoais, ilustrando origem e objetivos. Além disso, será analisado em específico o papel do direito europeu para formação dos conceitos contemporâneos de proteção de dados.

O segundo capítulo trará a composição do caso Cambridge Analytica e de suas repercussões. Serão estudados os antecedentes que contribuíram para o caso em estudo, bem como um enfoque na controvérsia-chave envolvendo a participação da empresa nas eleições presidenciais estadunidenses de 2016, culminando na urgência pela consolidação das legislações protetivas de dados ao redor do mundo, em especial no pioneirismo da *General Data Protection Regulation*, da União Europeia.

No terceiro capítulo, detalhar-se-á a Lei Geral de Proteção de Dados, bem como um enfoque nas características do direito à proteção de dados no Brasil. Além do corpo legislativo por si, será realizada uma análise comparativa com a legislação europeia a fim de identificar características presentes em ambos os institutos, bem como uma reflexão acerca da eficácia da LGPD na prevenção e combate a casos de violação como o ocorrido no objeto de estudo.

Com isso, o presente trabalho, além de analisar o histórico de dados pessoais enquanto instituto e entender a importância deste dentro do ordenamento jurídico brasileiro, propõe a reflexão sobre o papel e a influência do Direito Europeu

no conceito moderno de proteção de dados, bem como a consolidação de tais conceitos na legislação nacional, com o objetivo de identificar como o nosso ordenamento encontra-se posicionado a partir da perspectiva matriz europeia na capacidade de resolver e prevenir conflitos como o da Cambridge Analytica.

2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

O zelo acerca de dados e informações pessoais é algo que precede a modernização e as legislações específicas; afinal, a proteção de dados está intrinsecamente conectada ao conceito de privacidade. Resguardar as informações particulares é assegurar que uma parte da vida privada do indivíduo esteja amparada juridicamente, uma vez que tal conteúdo e sua eventual utilização indevida pode gerar danos ao seu proprietário.

No âmbito jurídico, as primeiras menções a esse instituto datam do século XIX. Sobre isso, Warren e Brandeis expandiram o direito à propriedade privada aos bens intangíveis.

> Gradualmente, o escopo desses direitos legais foi ampliado; e agora o direito à vida passou a significar o direito de aproveitar a vida - o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo "propriedade" cresceu para abranger todas as formas de posse - intangíveis, bem como tangíveis[1]. (Tradução nossa)

Essa concepção, ao apresentar o “direito de ser deixado em paz”, carrega uma visão passiva acerca do tema, manifestando-se apenas sobre a não intervenção do Estado na vida privada estendida aos aspectos não materiais. Todavia, com o passar do tempo, a mera proteção à privacidade associada à liberdade deixou de ser suficiente, dado o contexto e as possibilidades criadas pelas novas tecnologias. Para alcançar a efetividade, a noção de privacidade passou a requerer a capacidade do titular de pleitear seus direitos.

Ao se observar as definições mais modernas, Celso Ribeiro Bastos coloca a privacidade como a possibilidade de cada indivíduo de impedir o acesso ou a divulgação de informações sobre a vida privada, bem como a de afastar a intromissão de estranhos nessa seara[2]. Marcelo Cardoso Pereira, por sua vez, inclui o poder de controlar as informações pessoais dentro do conceito de direito à intimidade[3]. Ou seja,

---

[1] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard law review**, v. 4. 1890, p. 193.
[2] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, vol. 2, p. 63.
[3] PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 2ª ed. Curitiba: Juruá Editora, 2004, p.140.

no âmbito da privacidade, o Direito evoluiu para dar ao sujeito a capacidade ativa de reivindicar proteção sobre os dados dos quais é titular, não considerando apenas o cenário de não intervenção.

Na década de 1970, a tecnologia se desenvolvia e acentuava sua influência sobre o ambiente informacional, o que ampliava as possibilidades no que tange aos dados pessoais. O primeiro microprocessador foi criado em novembro de 1971 pela companhia estadunidense Intel, se tornando também o pioneiro na distribuição comercial. Nos anos seguintes, a empresa continuou desenvolvendo e lançando atualizações do seu produto, o que culminou no lançamento do computador pessoal Altair em 1974, cujo poder computacional superava em dez vezes a versão de três anos antes[4]. Percebe-se, então, que a informática sempre apresentou indícios de crescimento exponencial, o que impactaria a legislação e os direitos aos quais ela se relaciona.

Como destaca Danilo Doneda, esse período marca um aumento significativo da capacidade de coleta, processamento e uso da informação[5]. Isso, somado ao aumento da acessibilidade da tecnologia e o caráter doméstico que ela viria a assumir a partir de seu desenvolvimento e popularização, aumentou a influência que o tratamento de dados passou a ter na vida cotidiana. Com isso, o Direito precisou adaptar seus mecanismos para melhorar a eficiência frente ao novo cenário que se apresentava, visto que apenas a proteção negativa à privacidade já não era mais suficiente para abranger a particularidade dos dados pessoais.

Não obstante, a segunda metade do século XX marcou o surgimento das primeiras legislações especificamente voltadas à proteção de dados na União Europeia. Uma delas foi a lei de Land Hesse, promulgada na Alemanha nos anos 1970 e que, como destaca Joana de Moraes Souza Machado, tinha o objetivo de regular os bancos de dados informatizados do governo[6]. Sobre tal legislação, Ruaro e Rodriguez

---

[4] Primeiro processador do mundo, o Intel® 4004, comemora seu 40º aniversário. **Intel Newsroom**, 19 nov. 2011. Disponível em: https://newsroom.intel.com.br/news-releases/primeiro- processador-do-mundo-o-intel-4004-comemora-seu-40o-aniversario/#gs.7dqcem. Acesso em 1 ago. 2021.

[5] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. ed. Rio de Janeiro: Renovar, 2006, p. 12.

[6] MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre, RS: Editora Fi, 2018.

observam o surgimento do conceito da autodeterminação informativa a partir dessa iniciativa legal, reforçando a autonomia do indivíduo nesta relação jurídica.

> Este é o marco oficial em que surge da autodeterminação informativa, que seria, segundo a sentença, o direito dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados[7].

Na mesma época, a proteção de dados já vinha sendo alçada ao nível constitucional, dos quais se destacaram especialmente a Constituição Portuguesa de 1976 e a Constituição Espanhola de 1978. Os portugueses, além de atribuírem à lei a definição de dado pessoal, proibiam expressamente o acesso a dados de terceiros, salvo em casos excepcionais[8]. Do lado hispânico, estabeleceu-se que a lei restringiria o uso da informática com o objetivo de preservar a honra, a intimidade e o pleno exercício de direitos[9].

A partir de então, as legislações em torno do tema foram tomando cada vez mais corpo, especialmente na Europa, inspiradas nos casos concretos que não paravam de surgir e no posicionamento dos países vizinhos. O dever do Estado de resguardar a individualidade também no aspecto digital e de empoderar e conscientizar os cidadãos acerca da importância de gerir corretamente seus dados passou a ser representado em normas mais modernas e colocou a União Europeia como referência em proteção de dados a partir dos anos subsequentes.

2.1 Protagonismo do Direito Europeu

A proeminência da União Europeia e de seus estados membros na proteção à privacidade é destacada pelo engajamento dos países em iniciativas legislativas desde antes mesmo do Tratado de Roma. A Convenção Europeia dos Direitos Humanos de 1950, em seu artigo 8º, estabeleceu o “direito ao respeito pela vida

---

[7] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. **Revista Direito, Estado e Sociedade Programa de Pós-Graduação em Direito da PUC-Rio**, Rio de Janeiro, n. 36, p. 191-192. 12 set. 2010.

[8] “*Artigo 35º Utilização da informática. (...) 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. (...) 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.*” In PORTUGAL. Constituição Portuguesa de 1976.

[9] “*Artículo 18 (...) 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*.” In ESPANHA. Constituição Espanhola de 1978.

privada e familiar", colocando também restrições à atuação do ente público na ingerência sobre tal direito.

> Artigo 8º. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros[10].

Cabe destacar que todos os países-membros da União Europeia são signatários desta Convenção. Entretanto, embora manifestada a preocupação coletiva sobre a temática por iniciativa institucional do bloco, ainda havia um desnível entre as nações em termos de legislação específica.

Surgiu então a Diretiva nº 95/46/EC, aprovada em 1995, com o fito de regular o tratamento de dados pessoais e se tornar referência no âmbito europeu nesta matéria. Ela foi criada para ser um elemento essencial de privacidade e Direitos Humanos da União Europeia e se tornou um marco dentre as regulações do tema, consolidando um modelo legislativo que viria a inspirar as normas modernas que vigoram hoje em dia.

Como inovação, estabeleceu diversas definições importantes para uniformizar as interpretações e aplicações das leis, a exemplo do artigo 2º, que disciplina o entendimento do que é um dado pessoal, a base do direito à proteção de dados.

> Artigo 2º Para efeitos da presente directiva, entende-se por: a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social[11].

---

[10] UNIÃO EUROPEIA. Convenção Europeia dos Direitos Humanos. 4 nov 1950.

[11] UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 24/10/1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 10 ago. 2021.

O texto normativo estendia o escopo a qualquer processamento de dados, automatizado ou não. Além disso, o item 69 do preâmbulo da Diretiva estabelecia um prazo de três anos para que os países ajustassem a conformidade de suas normas com as novas diretrizes, além de estabelecer a implementação progressiva das práticas a tratamentos de dados que já estivessem em curso durante esse intervalo temporal[12].

A Diretiva preocupou-se não apenas em estabelecer os limites aplicáveis aos casos concretos, mas também incorporou princípios ao texto para as futuras condutas e legislações próprias sobre a matéria. O princípio da finalidade (art. 6º, item 1) e da legitimidade do processamento de dados delimitaram a ação das instituições responsáveis pelo tratamento de informações, assegurando também as garantias básicas do titular ao longo dos demais artigos[13].

O Capítulo IV da Diretiva 95/46/EC tratou especificamente da transferência de dados para países terceiros, mostrando estar à frente do seu tempo e antevendo um cenário global conturbado de dados compartilhados, mas sob jurisdições e práticas conflitantes. Prova disso é que, no decorrer dos anos, a União Europeia desenvolveu diversas estruturas para fluxo de dados para países fora do bloco. Um deles, o *Privacy Shield*, era uma colaboração entre UE e EUA para proteger os dados pessoais dos europeus e garantir a cooperação dos órgãos de comércio americanos com as autoridades europeias de proteção de dados[14].

O *Privacy Shield* substituiu o programa anterior, chamado *Safe Harbor*, após a declaração de invalidade deste pela Corte de Justiça da União Europeia em decisão de 2015, no caso *Maximillian Schrems v. Data Protection Commissioner*. Na ocasião, um cidadão austríaco, que possuía uma conta no Facebook, representou em razão de seus dados estarem sendo transferidos dos servidores subsidiários na Irlanda para serem processados nos EUA.

---

[12] Ibidem.
[13] Ibidem.
[14] COMISSÃO EUROPEIA. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. **Press Release**, Estrasburgo, 02 fev. 2016. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216. Acesso em 10 ago. 2021.

Dois anos antes deste julgamento, houve o famoso episódio de *whistleblowing* de Edward Snowden. O ex-funcionário da Agência Central de Inteligência (CIA) dos Estados Unidos denunciou as iniciativas de vigilância e monitoramento por parte dos serviços de inteligência americanos, especialmente da Agência de Segurança Nacional (NSA), à vida privada dos cidadãos e residentes no país, reflexo ainda do *USA Patriot Act* como resposta aos ataques de 11 de setembro e visando a prevenção de novos ataques terroristas. Através do programa PRISM, o governo estadunidense tinha acesso direto ao banco de dados de diversas empresas de tecnologia, dentre elas o Facebook, o que permitia a extração de e-mails, fotos, documentos e registros de conexão para rastreamento do usuário[15].

Dessa forma, a transferência de dados do usuário da Irlanda para os Estados Unidos representava a exposição daquelas informações pessoais a práticas não seguras quanto à preservação da privacidade. Por essa razão, a decisão da Corte Europeia mencionou o comprometimento deste direito ao invalidar a cooperação entre o bloco e os EUA.

> O Tribunal observa que a legislação que não prevê qualquer possibilidade de um indivíduo recorrer a soluções judiciais para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou apagamento de tais dados, compromete a essência do direito fundamental à eficácia judicial protecção, sendo a existência dessa possibilidade inerente à existência do Estado de direito[16].

Ainda, a própria Diretiva 95 deixa claro em seu artigo 25 que a transferência de dados pessoais para um país terceiro só pode ocorrer se este garantir um nível adequado de proteção dos dados[17], inclusive incumbindo à Comissão Europeia a revisão e a certificação das práticas dos demais países. Os Estados Unidos, quando

---

[15] GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. **The Washington Post**, Washington, 7 de jun. de 2013. Disponível em: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine- us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1. Acesso em 5 ago. 2021.

[16] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. **Press Release nº 177/15**, Luxemburgo, 6 out 2015. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. Acesso em 05 ago 2021.

[17] *Artigo 25º 1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objecto de tratamento, ou que se destinem a ser objecto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente directiva, o país terceiro em questão assegurar um nível de protecção adequado.* In: UNIÃO EUROPEIA, 1995.

da vigência do programa PRISM, claramente não se enquadravam no padrão legislativo vislumbrado pela Diretiva; portanto, a Corte decidiu pela suspensão da transferência dos dados daquele usuário para os EUA.

Nesse contexto, o *Privacy Shield*, em substituição ao *Safe Harbor*, veio como uma forma de controlar ainda mais essas interações do bloco com países estrangeiros em termos de tratamento de dados. O novo programa foi criado como uma certificação que impunha obrigações maiores sobre companhias nos EUA visando a proteção dos dados de cidadãos europeus. Além disso, um dos principais objetivos era clarificar também as obrigações do governo estadunidense em relação ao acesso às informações, estabelecendo limitações claras e instituindo vistorias anuais das práticas com atuação conjunta da Comissão Europeia e do Departamento de Comércio dos EUA[18].

Todavia, mesmo com as fiscalizações ainda mais cerradas sob o novo modelo, foi durante a vigência do *Privacy Shield* que ocorreu o grande escândalo da Cambridge Analytica, em que a empresa de análise de dados utilizou indevidamente informações de cerca de 50 milhões de usuários, obtidas por meio do Facebook, para análises de eleitorado na campanha de Donald Trump à presidência dos Estados Unidos[19]. Apesar dos esforços constantes e contínuos em estabelecer melhores práticas ao tratamento de dados, ainda havia a necessidade de uma legislação mais robusta e influente do que as tentativas anteriores.

---

[18] COMISSÃO EUROPEIA. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. **Press Release**, Estrasburgo, 02 fev. 2016. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216. Acesso em 10 ago. 2021.

[19] Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**, 20 mar. 2011. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em 11 ago. 2021.

3 O CASO CAMBRIDGE ANALYTICA

O modelo de negócios do Facebook, para que a plataforma se mantivesse gratuita e acessível, foi estruturado de forma que os anúncios representassem a principal fonte de receitas da plataforma[20]. Para isso, tais anúncios precisavam ser segmentados de acordo com o público-alvo, para que os anunciantes interessados pudessem se beneficiar tanto de uma projeção na escala que o meio digital permite, ao mesmo tempo que direcionada para aumentar as taxas de conversão.

> Assim, com base em quais páginas as pessoas gostam, em que clicam e em outros sinais, criamos categorias - por exemplo, pessoas que gostam de páginas sobre jardinagem e moram na Espanha - e cobramos dos anunciantes para exibir anúncios nessa categoria. Embora a publicidade para grupos específicos já existisse bem antes da Internet, a publicidade on-line permite uma segmentação muito mais precisa e, portanto, anúncios mais relevantes[21]. (tradução nossa)

Dessa forma, além dos dados que são inseridos na plataforma ao criar seu perfil, como nome, idade, local de residência, dentre outros, o Facebook também se utiliza de ferramentas terceiras para obter informações adicionais acerca do usuário – localização GPS do aparelho celular, rastreadores de interações em sites parceiros, etc. - da mesma forma que compartilha dados em alguma extensão com desenvolvedores e anunciantes. Todo esse volume de informações gera um largo banco de dados que incluem características e comportamentos dos consumidores, sendo esse alto volume de informações armazenadas pelas empresas hoje referenciado como *big data*.

Em 2010, o Facebook lançou a plataforma *Open Graph*, que permitia a desenvolvedores terceiros solicitarem permissão aos usuários para acessar dados pessoais deles e de seus amigos na rede social, incluindo nome, gênero, localização, além de preferências políticas e visões religiosas por meio da visualização de suas “curtidas”. O lançamento foi acompanhado por questionamentos acerca da privacidade e da utilização dos dados coletados, que ensejaram um artigo-resposta de Mark Zuckerberg publicado no The Washington Post em maio daquele ano:

---

[20] ZUCKERBERG, Mark. Understanding Facebook’s Business Model. **Meta**, 24 de jan. de 2019. Disponível em: https://about.fb.com/news/2019/01/understanding-facebooks-business-model/ Acesso em 25 nov. 2022.

[21] Ibidem.

> Ouvimos o feedback. Precisa haver uma maneira mais simples de controlar suas informações. Nas próximas semanas, adicionaremos controles de privacidade que são muito mais simples de usar. Também lhe daremos uma maneira fácil de desativar todos os serviços de terceiros. [...] Também ouvimos dizer que algumas pessoas não entendem como suas informações pessoais são usadas e se preocupam que sejam compartilhadas de maneiras que não querem[22]. (tradução nossa)

Três anos mais tarde, o Dr. Aleksandr Kogan, pesquisador do departamento de Psicologia da Universidade de Cambridge especializado em modelagem computacional de traços psicológicos, lançava como parte de sua pesquisa o aplicativo "*thisisyourdigitallife*" – Esta É Sua Vida Digital, em tradução livre. O aplicativo funcionava como um teste básico de personalidade, mas o usuário concordava em ter dados coletados e utilizados para fins acadêmicos. Em 2014, o aplicativo foi reposicionado para atender fins comerciais com a criação por Kogan de uma empresa chamada *Global Science Research* (GSR), sendo relançado com novos termos de uso[23].

Uma vez que a *Open Graph* permitia não apenas o acesso aos dados do usuário, mas também de amigos, o aplicativo conseguia explorar a permissão para gerar um efeito exponencial na coleta de informações, muito embora a política do Facebook não permitisse a venda ou uso comercial dos dados de amigos[24]. A interação de uma pessoa com a pesquisa representava em média a obtenção de informações sobre 300 usuários do Facebook[25]. No geral, estima-se que o banco de dados do aplicativo tenha acumulado dados de cerca de 87 milhões de pessoas através da interação de 270 mil usuários[26].

---

[22] ZUCKERBERG, Mark. From Facebook, answering privacy concerns with new settings. **The Washington Post**, Washington, 24 de mai. de 2010. Disponível em: https://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html Acesso em 25 nov. 2022.

[23] Statement from the University of Cambridge about Dr Aleksandr Kogan. **Cambridge University**, 11 de abr. de 2018. Disponível em: https://www.cam.ac.uk/notices/news/statement-from-the-university-of-cambridge-about-dr-aleksandr-kogan Acesso em 25 nov. 2022.

[24] CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, Grã-bretanha, 17 de mar. de 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election Acesso em 25 nov. 2022.

[25] WYLIE, Christopher. MINDF*CK: Cambridge Analytica and the Plot to Break America. Nova Iorque: Random House, 2019.

[26] KANG, Cecilia, FRENKEL, Sheera. Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. **The New York Times**, Nova Iorque, 4 de abr. de 2018. Disponível em: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html Acesso em 25 nov. 2022.

3.1 Atuação nas eleições presidenciais estadunidenses de 2016

A Cambridge Analytica foi uma firma de consultoria política criada em 2013 por executivos do mercado de *research* e comunicação estratégica. Sua atuação principal envolvia a criação de perfis psicográficos de eleitores para adaptar a comunicação de campanha às características do eleitorado-alvo, mimetizando estratégias de anunciantes comerciais para segmentar conteúdo político e, segundo Alexander Nix, então CEO da Cambridge Analytica, alinhar a campanha aos requisitos, desejos e necessidades dos eleitores[27].

Já em 2014, a companhia havia trabalhado no desenvolvimento de anúncios televisivos para políticos estadunidenses nas eleições parlamentares. Os anúncios eram produzidos e exibidos de forma personalizada aos eleitores conforme sua personalidade e propensão a assisti-los. Entretanto, o envolvimento da consultoria com a política foi inicialmente percebido de forma pública em 2015, quando o jornal britânico *The Guardian* reportou o uso de dados por parte da firma para modelagem de traços de personalidade de eleitores americanos[28], num esforço vinculado à campanha de Ted Cruz nas primárias do Partido Republicano para as eleições presidenciais estadunidenses do ano seguinte.

Em 2018, diversos veículos internacionais reportaram a aquisição de dados originários do Facebook por parte da Cambridge Analytica a partir da colaboração com a GSR, de Alexandr Kogan. As informações vieram a público a partir de Christopher Wylie, que trabalhou junto a Kogan na obtenção dos dados e denunciou à imprensa a coleta e utilização indevida de dados de cidadãos dos EUA para direcionamento de anúncios eleitorais[29].

---

[27] Cambridge Analytica. **Applying Data Science to Political Campaigns**. YouTube, 13 de ago. de 2015. Disponível em: https://www.youtube.com/watch?v=c_SlD7D_xug Acesso em 25 nov. 2022

[28] DAVIES, Harry. Ted Cruz using firm that harvested data on millions of unwitting Facebook users. **The Guardian**, 11 de dez. de 2015. Disponível em: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data Acesso em 25 nov. 2022.

[29] CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. How Trump Consultants Exploited the Facebook Data of Millions. **The New York Times**, 17 de mar. de 2018. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html Acesso em 25 nov. 2022.

Steve Bannon, conselheiro político que viria a ser diretor-executivo da campanha de Donald Trump à presidência dos EUA em 2016, possuía ligações com a consultoria na posição de investidor e conselheiro[30]. As estratégias aplicadas por Bannon e pela Cambridge Analytica na campanha que culminou com a vitória de Trump incluíam a exibição de campanhas personalizadas em diversas mídias alternando a exibição de Trump ou de celebridades, a depender do nível de alinhamento que o eleitor demonstrava com o candidato. Também foram implementadas publicidades direcionadas nas ferramentas de pesquisa, garantindo que a busca por palavras-chave negativas a Trump retornasse resultados favoráveis à campanha[31].

Apesar das estratégias em si não serem ilegais, a controvérsia foi gerada por esta ter sido habilitada com a utilização de dados de usuários coletados a partir de uma quebra da política de dados do Facebook, que inicialmente permitia a coleta pela ferramenta de Aleksandr Kogan para fins acadêmicos.

Em resposta, o Comitê Judiciário do Senado dos EUA promoveu uma investigação e convocou diversos envolvidos para depoimentos acerca do compartilhamento indevido de dados. O CEO do Facebook, Mark Zuckerberg, alegou perante ao Senado ter tomado conhecimento da condição de utilização dos dados apenas em 2015, quando solicitou a Kogan que estes fossem apagados[32]. O valor de mercado do Facebook à época se desvalorizou em mais de 119 bilhões de dólares nos dias subsequentes à publicação da controvérsia[33].

Em 2021, o Facebook fechou um acordo de 5 bilhões de dólares com a Comissão Federal de Comércio dos EUA em processo referente ao caso. No ano

---

[30] Ibidem.

[31] HILDER, Paul; LEWIS, Paul. Leaked: Cambridge Analytica's blueprint for Trump victory. **The Guardian**, 23 de mar. de 2018. Disponível em: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory Acesso em 25 nov. 2022.

[32] Facebook Inc. Documento à Câmara dos Representantes dos Estados Unidos da América, 29 de jun. de 2018. Disponível em: https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf Acesso em 25 nov. 2022

[33] NEATE, Rupert. Over $119bn wiped off Facebook's market cap after growth shock. **The Guardian**, 26 de jul. de 2018. Disponível em: https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock Acesso em 25 nov. 2022.

seguinte, outro acordo com valores não divulgados foi selado em processo indenizatório movido por um grupo de usuários do Facebook[34].

A mesma fonte foi responsável por informações relativas ao engajamento da Cambridge Analytica no *Brexit*, o plebiscito pela permanência ou não do Reino Unido na União Europeia em 2016. A companhia foi consultora política do grupo Leave.EU, favorável à saída do Reino Unido da UE[35]. Documentos da Cambridge Analytica também revelaram a atuação da consultoria em países como Rússia, Lituânia, Letônia, Ucrânia, Irã e Moldávia[36].

3.2 A Criação da *General Data Protection Regulation* (GDPR)

A GDPR nasceu de um esforço para atualizar as demais legislações vigentes, amplificando o movimento regulatório do qual o bloco europeu já era o protagonista. Em 2011, a Autoridade Europeia para a Proteção de Dados emitiu parecer intitulado "uma abordagem global da proteção de dados pessoais na União Europeia", cujo objetivo principal era a proposta de emenda à Diretiva 95/46/CE:

> A tecnologia atual não é a mesma que existia quando a Directiva 95/46/CE foi concebida e adotada. Fenômenos tecnológicos como a computação em nuvem, a publicidade comportamental, as redes sociais, a cobrança de portagens nas auto-estradas e os dispositivos de localização geográfica vieram alterar profundamente a forma como os dados são tratados e colocam enormes desafios à protecção de dados. A revisão das normas europeias nesta matéria terá de responder eficazmente a esses desafios[37].

---

[34] TOWNSEND, Mark. Facebook-Cambridge Analytica data breach lawsuit ends in 11th hour settlement. **The Guardian**, 27 de ago. de 2022. Disponível em: https://www.theguardian.com/technology/2022/aug/27/facebook-cambridge-analytica-data-breach-lawsuit-ends-in-11th-hour-settlement Acesso em 25 nov. 2022.

[35] What are the links between Cambridge Analytica and a Brexit campaign group? **Reuters**, 21 de mar. de 2018. Disponível em: https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu-idUSKBN1GX2IO Acesso em 25 nov. 2022.

[36] CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. **The Guardian**, 7 de mai. de 2017. Disponível em: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy Acesso em 25 nov. 2022.

[37] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS. "Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – «Uma Abordagem Global da Proteção de Dados Pessoais na União Europeia»". **Jornal Oficial da União Europeia**, 2011, nº C 181 de 22 de junho. Disponível em: https://edps.europa.eu/sites/default/files/publication/11-01-14_personal_data_protection_pt.pdf. Acesso em 14 ago 2021.

O parecer já destacava a evolução tecnológica desde a Diretiva 95 e foi acompanhada nos anos subsequentes de outros documentos e pareceres que encaminharam o processo para a concepção da GDPR em sua primeira versão, tanto sob a ótica de proteção jurídica quanto do bloco estar mais preparado economicamente para as transformações digitais. Já em 2012, a GDPR foi proposta pela Comissão Europeia ao Conselho da União Europeia como uma reforma estrutural na legislação de 1995, com destaque para a necessidade de organizações estabelecidas fora da UE, que prestassem serviços ou monitorassem indivíduos da UE, terem que designar um representante local. Além disso, houve a preocupação inicial com a definição para termos contemporâneos que não eram abarcados pela Diretiva 95:

> Algumas definições foram transpostas da Diretiva 95/46/CE, enquanto outras foram alteradas ou completadas por elementos suplementares ou novos (sobre «violação de dados pessoais», [...] «dados genéticos», «dados biométricos», «dados relativos à saúde», «estabelecimento principal», «representante», «empresa», «grupo de empresas», «regras vinculativas para empresas» e «criança», [...] e «autoridade de controlo»).[38]

Cabe destacar que o Parlamento Europeu havia ganhado destaque a partir de 2009, com a entrada em vigor do Tratado de Lisboa, que sucedeu os de Maastricht, Amsterdã e Nice. A partir destes, o Parlamento teve suas competências legislativas aumentadas consecutivamente e passou a ter poderes para aprovar, rejeitar e propor alterações a propostas legislativas a partir do novo Processo Legislativo Ordinário, detalhado em seu Regimento Interno[39].

Nisso, a proposta de 2012 da GDPR foi votada e aprovada pelo Parlamento Europeu em março de 2014. O parecer do Parlamento já destacava emendas a pontos relevantes da proposta, especialmente quanto ao consentimento para o processamento de dados pessoais para finalidades específicas e a necessidade de

---

[38] UNIÃO EUROPEIA. Comissão Europeia. Dossiê interinstitucional: 2012/0011 (COD). Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). Disponível em: https://data.consilium.europa.eu/doc/document/ST-5853-2012-INIT/pt/pdf Acesso em 14 ago 2021.

[39] UNIÃO EUROPEIA. Parlamento Europeu. Regimento do Parlamento Europeu, art 47 a 49. Disponível em: https://www.europarl.europa.eu/doceo/document/RULES-9-2022-07-11_PT.pdf Acesso em 25 nov. 2022

distinção clara entre cláusulas para consentimento de diferentes matérias, sob pena de nulidade:

> Artigo 7.º Condições para o consentimento
>
> 1. Quando o tratamento se basear no consentimento, incumbe ao responsável pelo tratamento o ónus de provar o consentimento do titular dos dados ao tratamento dos seus dados pessoais para finalidades específicas.
>
> 2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outra matéria, a exigência do consentimento deve ser apresentada de uma forma que a distinga claramente dessa outra matéria. As cláusulas relativas ao consentimento do titular dos dados que violem parcialmente este regulamento são consideradas nulas.
>
> 3. Não obstante outros fundamentos jurídicos para o tratamento, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Deve ser tão fácil retirar o consentimento como dá-lo. O titular dos dados deve ser informado pelo responsável pelo tratamento se a retirada do consentimento puder dar lugar à rescisão dos serviços fornecidos ou da relação com o responsável pelo tratamento.[40]

Assim, avançando no processo legislativo europeu, em 2015 a Autoridade Europeia para a Proteção de Dados (AEPD) publicou as recomendações para o texto final da GDPR[41], incluindo solicitações para que as autoridades de proteção de dados da UE estivessem preparadas para receber e investigar denúncias apresentadas pelos titulares dos dados, bem como ressaltando a necessidade de um sistema eficaz de responsabilização pelo tratamento ilícito de dados. Ademais, incluiu-se na recomendação um destaque especial para a necessidade da justificativa e do embasamento legal de forma simultânea para habilitar o tratamento de dados:

> 1.2. Todo o tratamento de dados deve ser simultaneamente lícito e justificado
>
> – As exigências de que todo o tratamento de dados seja limitado a fins específicos e tenha uma base jurídica são cumulativas, não alternativas. Recomendamos que se evite qualquer fusão destes princípios e o seu consequente enfraquecimento. Em vez disso, a UE deve preservar, simplificar

---

[40] UNIÃO EUROPEIA. Parlamento Europeu. Posição do Parlamento Europeu aprovada em primeira leitura em 12 de março de 2014 tendo em vista a aprovação do Regulamento (UE) n.º .../2014 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). Disponível em: https://www.europarl.europa.eu/doceo/document/TC1-COD-2012-0011_PT.pdf Acesso em 25 nov. 2022

[41] AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS. “Recomendações da AEPD sobre as opções da União Europeia para a reforma da proteção de dados”. **Jornal Oficial da União Europeia**, 2015, nº C 301/1 de 19 de setembro. Disponível em: https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_summary_pt_0.pdf Acesso em 14 ago 2021.

> e operacionalizar a ideia estabelecida de que os dados pessoais devem ser utilizados unicamente de forma compatível com as finalidades para que foram inicialmente recolhidos[42].

O texto final da GDPR foi publicado como ato legislativo do Parlamento Europeu e do Conselho Europeu, passando a vigorar em relação aos países-membros a partir de 25 de maio de 2018[43]. Nele, consta uma ampla lista de definição de termos no artigo 4º, os princípios relativos ao tratamento de dados pessoais, além da atenção às recomendações da AEPD quanto às punições cabíveis em caso de descumprimento, incluindo a possibilidade de multas de até 20 milhões de euros conforme previsão do artigo 83, § 4º.

Dentre os termos definidos pelo texto legislativo, cabe destacar as definições de “tratamento”, “responsável pelo tratamento” e “consentimento”, e em especial a definição de “dados pessoais” trazida pelo regulamento, que seria pauta nas legislações subsequentes inspiradas na GDPR:

> Artigo 4º Definições
>
> Para efeitos do presente regulamento, entende-se por:
>
> 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;[44]

Outro destaque é a necessidade estabelecida pelo artigo 37 da designação de um encarregado da proteção de dados por parte do responsável pelo tratamento, seja este responsável um agente público ou privado, sempre que houver necessidade de controle e/ou tratamento de dados em grande escala em decorrência das atividades desempenhadas. O *Data Privacy Officer*, segundo o mesmo artigo, poderia ser um

---

[42] Idem. Item 1.2

[43] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016, nº L 119/1 de 4 de maio. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679 Acesso em 25 nov. 2022

[44] Ibidem.

prestador de serviços terceiro, o que criou um novo mercado para que indivíduos e empresas pudessem se especializar para ocupar essas funções.

Também ficou estabelecida, no artigo 51, a responsabilidade de autoridades públicas independentes para fiscalizar e aplicar o regulamento. A independência da autoridade de controle ficou ilustrada no artigo seguinte:

> Artigo 52. Independência
>
> 2. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem.
>
> 6. Os Estados-Membros asseguram que cada autoridade de controlo fique sujeita a um controlo financeiro que não afeta a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional.[45]

Apesar de o processo de atualização legislativa e elaboração da GDPR vir sendo conduzido desde 2012, a publicização do caso Cambridge Analytica em março de 2018 impulsionou a aprovação e a entrada em vigor poucos meses depois no mesmo ano. Percebe-se, ainda, que diversas previsões que seriam aplicáveis àquele caso já estavam presentes no texto legal, tanto na definição de dados pessoais quanto na responsabilização sobre o processamento de dados para utilização específica, além da necessidade de consentimento direcionado para cada aplicação, o que ressalta a capacidade dos legisladores europeus em antever cenários de crise na privacidade de dados pessoais.

---

[45] Ibidem.

4 A LEI Nº 13.709/2018 NA PROTEÇÃO DE DADOS NO BRASIL

No Brasil, apesar da previsão constitucional de inviolabilidade do sigilo de dados no artigo 5º, XII[46], decorrente do processo de redemocratização, a discussão moderna acerca da proteção de dados pessoais no Brasil ganha tração a partir de 2010, quando da Consulta Pública sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, realizada pelo Ministério da Justiça e encerrada em 2011.

A partir disso, iniciou-se uma discussão legislativa para elaboração de Lei que incorporasse os movimentos jurídicos observados nos demais países, com influência especial do Direito Europeu, para que fossem positivados os direitos à proteção de dados dentro de características pertinentes às situações atuais. Com isso, foi proposto o Projeto de Lei 4.060/12 pelo então Deputado Federal Milton Monti para dispor sobre o tratamento de dados pessoais[47], projeto este que viria a se tornar a Lei Geral de Proteção de Dados posteriormente.

Dentro de sua justificativa, o projeto já apresentava a necessidade de proteger a individualidade e a privacidade, sem inviabilizar a livre iniciativa e a comunicação – mecanismos essenciais a serem preservados dentro do avanço tecnológico. Ademais, além do que já se podia perceber pelos dispositivos legais inseridos no então Projeto de Lei supracitado, a inspiração na GDPR ficou evidente no discurso da Deputada Bianca Furlan, então Parlamentar Federal por São Paulo e presidente da Comissão Especial daquele Projeto de Lei, à Câmara Federal em junho de 2018:

> A União Europeia mostrou-se especialmente atenta à matéria, implantando lei modelar de proteção dos dados pessoais. A legislação europeia se destaca por um juízo de ponderação, baseado em parâmetros como “necessidade” e “proporcionalidade”, de modo a equilibrar o interesse privado e o interesse público. Tais conceitos serviram de inspiração para o trabalho desenvolvido no

---

[46] ”é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”. In: BRASIL. Constituição da República Federativa do Brasil de 1988.

[47] BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 4.060/2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01lviv46xz0k1o1eo8x27hqa5jv689234.node0?codteor=1001750&filename=PL+4060/2012 Acesso em 25 nov. 2022

> âmbito da Comissão Especial do PL 4.060/12 e apensado, que tive a honra de presidir.[48]

O Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, sob a premissa de estabelecer direitos e deveres para o uso da Internet no Brasil, foi uma das primeiras legislações a abordar a proteção de dados pessoais dos usuários no Brasil sob a ótica das relações digitais. Destaca-se o artigo 7º, incisos VII e IX, que protegem o usuário quanto à coleta, utilização e tratamento, bem como já estabelecem a necessidade de consentimento expresso para tal, elementos que serviriam também de base para a legislação específica de proteção de dados que viria posteriormente.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> [...]
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Com o escândalo da Cambridge Analytica sendo divulgado em 2008, seguido pela entrada em vigor da GDPR, o Brasil avançou no trâmite do Projeto de Lei 4.060/12, que viria a ser aprovado em agosto de 2018 e revertido na Lei nº 13.709/2018 – a Lei Geral de Proteção de Dados (LGPD). Todavia, a preocupação com a adequação das empresas e instituições às disposições da nova lei ensejou diversos adiamentos em sua entrada em vigor. O período que era inicialmente de 18 meses da publicação foi alterado para 24 meses pela Lei nº 13.853/2019[49], seguida

---

[48] BRASIL. Câmara dos Deputados. **Diário da Câmara dos Deputados**. Brasília: Câmara dos Deputados, 2018, p. 155. Disponível em: http://imagem.camara.gov.br/Imagem/d/pdf/DCD00201806060008500000.PDF Acesso em 25 nov 2022.

[49] 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: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm Acesso em 25 nov 2022.

por nova alteração a partir da Lei nº 14.010/2020, que dispôs entrada em vigor a partir do dia 1 de agosto de 2021 quanto aos artigos referentes à fiscalização e às sanções administrativas aplicáveis[50].

Além do objetivo principal de proteção dos direitos fundamentais de liberdade e privacidade, a LGPD trouxe como características a definição de dados pessoais, especificando pontos como dados sensíveis e dados sobre crianças e adolescentes como elementos que ensejam proteção especial, além de posicionar o consentimento como elemento indispensável para o tratamento de dados, seguindo a linha da legislação internacional até então.

Ademais, a previsão de uma agência reguladora na LGPD deu origem à Autoridade Nacional de Proteção de Dados (ANPD), criada a partir da Lei nº 13.853/2019 com o fito de orientar e regular a aplicação da LGPD[51], além de fiscalizar e aplicar as sanções em caso de descumprimento legal. Ainda, por determinação da mesma lei a ANPD ficou responsável por deliberar administrativamente sobre a interpretação da LGPD, suas competências e casos omissos.

4.1 Um estudo comparativo entre a GDPR e a legislação brasileira

Apesar de apresentarem estrutura semelhante, a LGPD e a GDPR apresentam diferenças destacáveis quanto a seus institutos e ao grau de especificidade conferido a cada um deles. No âmbito das definições, a lei brasileira traz uma abordagem direta para terminologias como “dados pessoais”, “dados pessoais sensíveis”. Nestes, observa-se na lei brasileira uma opção pela definição ampla. Ao dispor, por exemplo, dado pessoal apenas como “informação relacionada a pessoa natural identificada ou identificável” em seu artigo 5º, inciso I, opta-se por um caminho diferente da lei europeia, que indica em rol exemplificativo as possibilidades de enquadro como dado

---

[50] BRASIL. **Lei Nº 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm Acesso em 25 nov 2022.

[51] 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: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm Acesso em 25 nov 2022.

pessoal – nome, número de identificação, dados de localização, elementos da identidade fisiológica, dentre outros.

Apesar de no inciso seguinte a LGPD ser mais específica quanto às possibilidades de dados pessoais sensíveis, citando situações como dados relacionados à saúde, dados genéticos ou biométricos, dentre outros, percebe-se que a GDPR, ainda que apresente definições específicas também sobre estes, os enquadra como dados pessoais já em caráter amplo.

Aqui, a atenção especial volta-se a um ponto: a GDPR esclarece que pessoa identificável se trata da pessoa que "possa ser identificada, direta ou indiretamente, em especial por referência a um indicador". Este ponto é especialmente importante por se relacionar com o conceito do dado anonimizado na LGPD (artigo 5º, inciso III) ou pseudonimização na GDPR (artigo 4º, item 5). A pseudonimização, para a lei europeia, manifesta que informações suplementares, se mantidas separadas e com medidas aplicadas para que não sejam atribuídos a uma pessoa singular, deixam de ser atribuídos como pessoais. O conceito paralelo na LGPD é definido como o dado que não possa ser identificado, considerando a utilização dos meios técnicos disponíveis.

Ao correlacionar as duas definições, o par "dados pessoais" e "pseudonimização" da GDPR ilustra com clareza que o agente de tratamento de dados, ainda que possua informações sobre seu domínio que, em conjunto, possam ser enquadradas como pessoais em razão de tornar o sujeito identificável, tem a capacidade de administrá-los a fim de manter-se em conformidade com a norma.

> 5) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;[52]

[52] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016, nº L 119/1 de 4 de maio. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679 Acesso em 25 nov. 2022

Do ponto de vista brasileiro, as disposições conferem uma descrição relativa à natureza do dado (já que este é anonimizado pela definição, enquanto na GDPR a pseudonimização é ilustrada como processo). Ainda que a LGPD apresente também o conceito de anonimização em seu artigo 5º, inciso XI, este versa sobre utilização de meios disponíveis no meio do tratamento para que o dado perca a possibilidade de associação, mas ainda não toca na possibilidade de operação simultânea destes dados, ainda que de forma independente.

No âmbito do consentimento, outro instituto relevante na proteção de dados, a legislação brasileira o categoriza como uma concordância livre, informada e inequívoca do titular para o tratamento de seus dados para uma finalidade específica. Assim como na GDPR, há o destaque para a caracterização da liberdade, informação e especificidade deste consentimento. Em ambas as legislações, há a preocupação de que este não seja obtido de forma automática ou automatizada, ou mesmo pressuposta – por exemplo, a mera utilização ou engajamento em determinada plataforma não pode configurar um consentimento, tampouco o uso de ferramentas pré-preenchidas ou selecionadas.

O art. 8º da LGPD traz que o consentimento pode ser expresso pelo titular através de meios que demonstrem a manifestação de vontade, seja escrito ou outro. Assim, desde que a navegabilidade dos termos das plataformas conte com um mecanismo que requeira o engajamento expresso do titular, ainda que de forma digital, para a utilização na finalidade especificada, configura-se o consentimento. Exceções nos casos de dados pessoais sensíveis, que requerem destaque especial para que o consentimento seja configurado, e de crianças e adolescentes, cuja natureza do titular requer que o consentimento seja feito por um responsável legal, previsão que também é compartilhada com a GDPR. Ambas as leis também garantem o direito à retirada do consentimento a qualquer momento por parte do titular.

Outra diferença reside na questão dos dados sensíveis. A GDPR traz uma proibição expressa, em seu artigo 9º, do tratamento de categorias específicas de dados pessoais:

> Artigo 9.o
>
> Tratamento de categorias especiais de dados pessoais

> 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa[53]

Nesse caso, a GDPR opta por expressar a proibição para, em seguida, estabelecer casos de exceção em que o tratamento de dados pessoais dessas categorias se torna permitido – a exemplo da necessidade do tratamento de tais dados para defesa judicial ou exercício de direitos. Apesar de trazer hipóteses muito similares para habilitar o tratamento de dados pessoais sensíveis, a LGPD categoriza as situações em que o tratamento destes é autorizado, não trazendo a proibição no texto legal. Apesar da aplicação jurídica ser semelhante, a semântica da GDPR posiciona o tratamento de dados sensíveis como exceção, enquanto a escolha da LGPD opta pela delimitação positiva das possibilidades.

No âmbito do controle de riscos, outro comparativo que se destaca entre as legislações é a postura a ser adotada neste tipo de situação. A GDPR é clara ao estabelecer o instituto da Avaliação de Impacto em seu artigo 35, a ser realizada pelo responsável pelo tratamento de dados nos casos em que a operação possa implicar elevado risco para direitos e liberdades. Deve ser avaliada a necessidade e proporcionalidade do tratamento, os riscos envolvidos e as medidas mitigatórias de risco. A LGPD, por sua vez, traz o Relatório de Impacto como instituto, mas não estabelece o seu conteúdo ou as situações em que este deve ser elaborado de forma obrigatória, posicionando o instituto apenas como uma possibilidade a ser determinada pela autoridade nacional.

Já sobre as avaliações de impacto, se versa sobre situações em que o risco é iminente, mas ainda não ocorreu. Quanto aos casos de incidentes de segurança, em que houve falha no tratamento dos dados e o risco foi consumado em dano, a GDPR novamente é mais explícita ao estabelecer, em seu artigo 33, § 1º [54], a necessidade de notificação à autoridade competente no prazo de 72 horas. A LGPD, por sua vez,

---

[53] Ibidem.

[54] Idem. “Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.”

ainda que preveja a notificação às autoridades e ao titular pelo agente de tratamento de dados, coloca apenas que esta deve ser feita em prazo razoável no artigo 48, § 1º, trazendo um dispositivo menos específico.

4.2 A Prevenção ao Efeito Cambridge Analytica

A controvérsia do caso Cambridge Analytica parte da exploração do mecanismo de uma plataforma por parte de um terceiro para coletar e processar dados em alto volume. Tanto a Cambridge Analytica quanto o Facebook, à luz da LGPD, poderiam ser responsabilizados acerca da utilização indevida dos dados pessoais na ocasião.

Isto se deve pelo fato de, assim como na GDPR, a legislação brasileira incluir o controlador e o operador como agentes de tratamento. A lei assim define controladores e operadores:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;[55]

Pela narrativa do caso, resta claro que a consultoria prestada pela Cambridge Analytica foi feita a partir do tratamento de dados pessoais sensíveis, posto que as posições políticas dos cidadãos eram o principal interesse dos clientes que a firma auxiliava – na situação, instituições políticas, políticos e candidatos. Assim, tanto Aleksandr Kogan, criador do aplicativo que realizava a coleta e o tratamento de dados, quanto a Cambridge Analytica, o organismo controlador na tomada de decisões, poderiam ser enquadrados como sujeitos a serem responsabilizados.

Todavia, o Facebook, na posição de detentor originário dos dados sensíveis, uma vez que estes eram coletados a partir de sua plataforma, também é responsável pelas decisões referentes ao tratamento de dados pessoais. Afinal, a plataforma tem a prerrogativa de definir as circunstâncias em que os dados em sua posse serão

---

[55] BRASIL**. Lei Nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm Acesso em 25 nov 2022.

compartilhados, bem como controla o acesso de terceiros ao seu banco de dados, podendo ser caracterizada com controladora e, portanto, responsabilizada.

Ademais, o próprio tratamento destes dados sensíveis somente poderia ser desempenhado nas hipóteses específicas da lei e para finalidades nas quais o consentimento tenha sido expressamente solicitado. Há uma confusão clara no consentimento a partir do momento em que o projeto de coleta de dados por meio do aplicativo de Alexandr Kogan se inicia com objetivos acadêmicos e depois é transposto para fins comerciais. Logo, duas frentes permanecem abertas nessa problemática: a autorização dada pelo Facebook a partir da plataforma *Open Graph* para o compartilhamento desses dados com terceiros e a utilização destes por parte da Cambridge Analytica para fins comerciais.

A existência de uma legislação específica para estes casos influencia não apenas na caracterização do problema, mas também na própria resposta que será aplicada no caso concreto. Ambas as leis determinam a presença de profissionais capacitados nas organizações com o fito de manter a conformidade com a norma. O Data Privacy Officer (DPO) na legislação europeia ou o Encarregado pelo Tratamento de Dados Pessoais na lei brasileira são instrumentos que, se posicionados em organizações com tratamento de dados em larga escala com o Facebook, seriam capazes de reforçar o *compliance* quanto à proteção de dados e coordenar ações de forma mais eficiente, seja em caráter preventivo ou corretivo. Por exemplo, haveria a necessidade clara da notificação dos usuários por parte do Facebook acerca do comprometimento de seus dados pessoais antes que a situação fosse revelada em caráter público pelos veículos de imprensa.

Todavia, a construção do perfil psicológico dos eleitores por parte da Cambridge Analytica foi realizada a partir de um processamento altamente complexo dos dados pessoais. A partir de análises comportamentais e de interesses, a consultoria foi capaz de conferir prognósticos acerca da propensão de determinado indivíduo engajar com determinados posicionamentos políticos e ideológicos. Dessa forma, há o possível um cenário em que o agente de tratamento, a partir de inferências e da utilização de dados não-sensíveis, gere conclusões que seriam enquadradas como dados sensíveis – o que enseja a discussão sobre a forma com que estes são

conectados aos cidadãos e se podem ser considerados “pessoais” sob a ótica da LGPD a partir dessas associações.

CONSIDERAÇÕES FINAIS

As transformações tecnológicas geraram a necessidade de atualização legislativa para compor um mecanismo de proteção eficiente aos dados pessoais, num contexto de alto volume de processamento de informações. O caso Cambridge Analytica adquiriu conotação especial por colocar em evidências essa necessidade a partir de um incidente envolvendo o Facebook, uma das maiores plataformas de interação social dos dias atuais e que concentra uma quantidade incalculável de dados em seu domínio.

Ao analisarmos a proteção de dados e a privacidade desde a sua origem, com especial atenção à contribuição do direito europeu, pudemos verificar a evolução dos mecanismos jurídicos ao longo das épocas, bem como a abordagem utilizada para consolidar a *General Data Protection Regulation*, que viria a servir de base para as demais legislações ao redor do mundo, em especial a Lei Geral de Proteção de Dados no Brasil.

Assim, foi possível identificar que o nosso ordenamento, em especial a LGPD, embora carregue suas particularidades pertinentes ao ordenamento jurídico brasileiro, encontra-se posicionado de forma muito semelhante em diversos institutos nos quais a GDPR se fundamenta. Inclusive, o Brasil, assim com a União Europeia, mostrou comprometimento com a proteção de dados antes mesmo da eclosão da controvérsia relativa à Cambridge Analytica, tendo discutido a legislação desde 2012 e aprovando o texto final da LGPD poucos meses após a publicação da GDPR.

Ademais, analisando a legislação à luz do caso Cambridge Analytica, percebe-se a importância de uma codificação específica e da atribuição de previsões legais como a Agência Nacional de Proteção de Dados de forma ampla, e do *Data Privacy Officer* de forma específica, para participar de forma mais próxima da prevenção, fiscalização e correção dos demais dados. Todavia, sob a ótica do mesmo caso, foi possível identificar situações que ainda não são completamente abarcadas pelo texto legal, o que reforça a necessidade de constante atualização visando a preservação do direito à privacidade por meio da proteção dos dados pessoais.

Para isso, as informações detalhadas da ocasião, em especial as reportagens estrangeiras, foram essenciais para compreender o *modus operandi* da Cambridge Analytica e ilustrar a complexidade da situação, para assim entender as ramificações e implicações do caso dentro da legislação atual e potenciais ofensas futuras.

No mais, o tema da proteção de dados é algo que permeia o dia a dia moderno, razão pela qual se mostra em constante atualização. A LGPD ainda é objeto de estudo de diversos doutrinadores, e dada a sua entrada em vigor de forma completa apenas em caráter recente, certamente há espaço para expansão das reflexões sobre seu conteúdo, em especial na proteção dos cidadãos brasileiros quanto à segurança da informação e ao direito à privacidade na utilização de redes sociais.

REFERÊNCIAS

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS. “Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – «Uma Abordagem Global da Proteção de Dados Pessoais na União Europeia»”. Jornal Oficial da União Europeia, 2011, nº C 181 de 22 de junho. Disponível em: https://edps.europa.eu/sites/default/files/publication/11-01-14 _personal_data_protection_pt.pdf. Acesso em 14 ago 2021.

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS. “Recomendações da AEPD sobre as opções da União Europeia para a reforma da proteção de dados”. Jornal Oficial da União Europeia, 2015, nº C 301/1 de 19 de setembro. Disponível em: https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_summary_pt_0.pdf Acesso em 14 ago 2021.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo: Saraiva, 1989, vol. 2, p. 63.

BRASIL. Câmara dos Deputados. Diário da Câmara dos Deputados. Brasília: Câmara dos Deputados, 2018. Disponível em: http://imagem.camara.gov.br/Imagem/d/pdf/DCD0020180606000850000.PDF#page=155 Acesso em 25 nov 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei Nº 4.060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01lviv46xz0k1o1eo8x27hqa5jv689234.node0?codteor=1001750&filename=PL+4060/2012 Acesso em 25 nov. 2022

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm Acesso em 25 nov 2022.

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: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm Acesso em 25 nov 2022.

BRASIL. Lei Nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm Acesso em 25 nov 2022.

CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. The Guardian, 7 de mai. de 2017. Disponível em: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy Acesso em 25 nov. 2022.

CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. How Trump Consultants Exploited the Facebook Data of Millions. The New York Times, 17 de mar. de 2018. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html Acesso em 25 nov. 2022.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, Grã-bretanha, 17 de mar. de 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election Acesso em 25 nov. 2022.

Cambridge Analytica. Applying Data Science to Political Campaigns. YouTube, 13 de ago. de 2015. Disponível em: https://www.youtube.com/watch?v=c_SlD7D_xug Acesso em 25 nov. 2022

COMISSÃO EUROPEIA. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Press Release, Estrasburgo, 02 fev. 2016. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216. Acesso em 10 ago. 2021.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press Release nº 177/15, Luxemburgo, 6 out 2015. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. Acesso em 05 ago 2021.

DAVIES, Harry. Ted Cruz using firm that harvested data on millions of unwitting Facebook users. The Guardian, 11 de dez. de 2015. Disponível em: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data Acesso em 25 nov. 2022.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 1. ed. Rio de Janeiro: Renovar, 2006, p. 12.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. G1, 20 mar. 2011. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em 11 ago. 2021.

ESPANHA. Constituição Espanhola de 1978.

Facebook Inc. Documento à Câmara dos Representantes dos Estados Unidos da América, 29 de jun. de 2018. Disponível em:

https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf Acesso em 25 nov. 2022

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post, Washington, 7 de jun. de 2013. Disponível em: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine- us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1. Acesso em 5 ago. 2021.

HILDER, Paul; LEWIS, Paul. Leaked: Cambridge Analytica's blueprint for Trump victory. The Guardian, 23 de mar. de 2018. Disponível em: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory Acesso em 25 nov. 2022.

KANG, Cecilia, FRENKEL, Sheera. Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. The New York Times, Nova Iorque, 4 de abr. de 2018. Disponível em: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html Acesso em 25 nov. 2022.

MACHADO, Joana de Moraes Souza. A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil. Porto Alegre, RS: Editora Fi, 2018.

NEATE, Rupert. Over $119bn wiped off Facebook's market cap after growth shock. The Guardian, 26 de jul. de 2018. Disponível em: https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock Acesso em 25 nov. 2022.

PEREIRA, Marcelo Cardoso. Direito à intimidade na internet. 2ª ed. Curitiba: Juruá Editora, 2004, p.140.

PORTUGAL. Constituição Portuguesa de 1976.

Primeiro processador do mundo, o Intel® 4004, comemora seu 40º aniversário. Intel Newsroom, 19 nov. 2011. Disponível em: https://newsroom.intel.com.br/news-releases/primeiro- processador-do-mundo-o-intel-4004-comemora-seu-40o-aniversario/#gs.7dqcem. Acesso em 1 ago. 2021.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. Revista Direito, Estado e Sociedade Programa de Pós-Graduação em Direito da PUC-Rio, Rio de Janeiro, n. 36, p. 191-192. 12 set. 2010.

Statement from the University of Cambridge about Dr Aleksandr Kogan. Cambridge University, 11 de abr. de 2018. Disponível em: https://www.cam.ac.uk/notices/news/statement-from-the-university-of-cambridge-about-dr-aleksandr-kogan Acesso em 25 nov. 2022.

TOWNSEND, Mark. Facebook-Cambridge Analytica data breach lawsuit ends in 11th hour settlement. The Guardian, 27 de ago. de 2022. Disponível em:

https://www.theguardian.com/technology/2022/aug/27/facebook-cambridge-analytica-data-breach-lawsuit-ends-in-11th-hour-settlement Acesso em 25 nov. 2022.

UNIÃO EUROPEIA. Comissão Europeia. Dossiê interinstitucional: 2012/0011 (COD). Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). Disponível em: https://data.consilium.europa.eu/doc/document/ST-5853-2012-INIT/pt/pdf Acesso em 14 ago 2021.

UNIÃO EUROPEIA. Convenção Europeia dos Direitos Humanos. 4 nov 1950.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 10 ago. 2021.

UNIÃO EUROPEIA. Parlamento Europeu. Posição do Parlamento Europeu aprovada em primeira leitura em 12 de março de 2014 tendo em vista a aprovação do Regulamento (UE) n.º .../2014 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). Disponível em: https://www.europarl.europa.eu/doceo/document/TC1-COD-2012-0011_PT.pdf Acesso em 25 nov. 2022

UNIÃO EUROPEIA. Parlamento Europeu. Regimento do Parlamento Europeu, art 47 a 49. Disponível em: https://www.europarl.europa.eu/doceo/document/RULES-9-2022-07-11_PT.pdf Acesso em 25 nov. 2022

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016, nº L 119/1 de 4 de maio. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679 Acesso em 25 nov. 2022

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard law review, v. 4. 1890, p. 193.

What are the links between Cambridge Analytica and a Brexit campaign group? Reuters, 21 de mar. de 2018. Disponível em: https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu-idUSKBN1GX2IO Acesso em 25 nov. 2022.

WYLIE, Christopher. MINDF*CK: Cambridge Analytica and the Plot to Break America. Nova Iorque: Random House, 2019.

ZUCKERBERG, Mark. From Facebook, answering privacy concerns with new settings. The Washington Post, Washington, 24 de mai. de 2010. Disponível em:

https://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html Acesso em 25 nov. 2022.

ZUCKERBERG, Mark. Understanding Facebook’s Business Model. Meta, 24 de jan. de 2019. Disponível em: https://about.fb.com/news/2019/01/understanding-facebooks-business-model/ Acesso em 25 nov. 2022.