

UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL
FACULDADE DE DIREITO DE ALAGOAS – FDA
GRADUAÇÃO EM DIREITO

ANDERSON CAVALCANTE SANTOS

**RESPONSABILIDADE CIVIL NO INCIDENTE DE COMPARTILHAMENTO
INDEVIDO DE DADOS PESSOAIS EM PLATAFORMAS DIGITAIS À LUZ DA
LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/18): ANÁLISE DO
CASO FACEBOOK**

MACEIÓ – AL
2025

ANDERSON CAVALCANTE SANTOS

**RESPONSABILIDADE CIVIL NO INCIDENTE DE COMPARTILHAMENTO
INDEVIDO DE DADOS PESSOAIS EM PLATAFORMAS DIGITAIS À LUZ DA
LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/18): ANÁLISE DO
CASO FACEBOOK**

Trabalho de Conclusão de Curso
submetido ao corpo docente de
graduação em Direito de Alagoas (FDA),
unidade acadêmica da Universidade
Federal de Alagoas (UFAL), como
requisito parcial à obtenção do grau em
Bacharel em Direito.

Orientador: Prof. Me. Fernando Antônio
Barbosa Maciel

MACEIÓ – AL

2025

Catálogo na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

S586c Santos, Anderson Cavalcante.
Responsabilidade civil no incidente de compartilhamento indevido de dados pessoais em plataformas digitais à luz da Lei Geral de Proteção De Dados (lei nº 13.709/18) : análise do caso Facebook / Anderson Cavalcante Santos. – 2025.
63 f.

Orientador: Fernando Antônio Barbosa Maciel.
Monografia (Trabalho de Conclusão de Curso em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Maceió, 2025.

Bibliografia: f. 60-63.

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. Responsabilidade civil. 3. Dados pessoais. 4. Plataforma digital. 5. Facebook (Rede social *on-line*). 6. Cambridge Analytica (Firma). I. Título.

CDU: 342.738

Folha de Aprovação

ANDERSON CAVALCANTE SANTOS

RESPONSABILIDADE CIVIL NO INCIDENTE DE COMPARTILHAMENTO INDEVIDO DE DADOS PESSOAIS EM PLATAFORMAS DIGITAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/18): ANÁLISE DO CASO FACEBOOK

Esta monografia de conclusão de curso de graduação em Direito, apresentada à Faculdade de Direito de Alagoas (FDA/UFAL) como requisito parcial para a obtenção do grau de Bacharel em Direito, obteve a devida aprovação perante a presente banca examinadora em 09/06/2025.

FERNANDO ANTONIO
BARBOSA
MACIEL:82816760430

Assinado de forma digital por
FERNANDO ANTONIO BARBOSA
MACIEL:82816760430
Dados: 2025.06.10 18:25:30 -03'00'

Orientador – Prof. Me. Fernando Antônio Barbosa Maciel
(Universidade Federal de Alagoas)

Banca examinadora:

Documento assinado digitalmente
 **QUERINO MALLMANN**
Data: 09/06/2025 11:24:53-0300
Verifique em <https://validar.iti.gov.br>

Examinador Interno: Prof. Dr. Querino Mallmann
(Universidade Federal de Alagoas)

Documento assinado digitalmente
 **LAVINIA CAVALCANTI LIMA CUNHA**
Data: 10/06/2025 15:23:56-0300
Verifique em <https://validar.iti.gov.br>

Examinadora Interna: Profa. Ma. Lavínia Cavalcante Lima Cunha
(Universidade Federal de Alagoas)

AGRADECIMENTOS

Antes de tudo e acima de tudo, agradeço a Deus, o realizador dos meus sonhos e projetos, que em cada passo da minha caminhada me sustentou e me guiou até aqui.

Agradeço à minha família, minha base e alicerce em todos os momentos da vida. À minha esposa, Wiquelani Nunila, que esteve ao meu lado em cada desafio, me apoiando, incentivando e impulsionando a seguir em frente mesmo nas horas mais difíceis. À minha filha, Nicole Nunila, que com sua doçura e uma simples frase, “você consegue, papai”, renovava minhas forças e me dava combustível e energia para prosseguir.

Aos meus pais, Agnaldo e Gilzania, meus grandes apoiadores e exemplos de vida, que me ensinaram com amor e dedicação o valor da perseverança e do trabalho honesto.

Sou grato também ao Tribunal de Justiça de Alagoas, especialmente ao Juizado Especial Cível e Criminal de Rio Largo, onde tive o privilégio de estagiar nos últimos dois anos e tanto aprendi, não apenas sobre o Direito, mas sobre o compromisso com a Justiça e o serviço ao próximo.

Por fim, agradeço à Universidade Federal de Alagoas, minha segunda casa durante esses anos tão intensos, por todo o conhecimento transmitido, pelas amizades construídas e pela oportunidade de tornar este grande sonho em realidade.

A todos vocês, meu mais sincero obrigado.

RESUMO

O presente trabalho tem como objetivo analisar a responsabilidade civil das plataformas digitais diante do compartilhamento indevido de dados pessoais, à luz da Lei Geral de Proteção de Dados (Lei nº 13.709/18), utilizando como estudo de caso o escândalo envolvendo o Facebook e a consultoria britânica Cambridge Analytica. O caso, amplamente noticiado pela mídia internacional, revelou que a rede social permitiu, por meio de um aplicativo externo, o acesso a dados de até 87 milhões de usuários, sem o consentimento informado e específico desses titulares. No Brasil, estima-se que cerca de 443 mil usuários foram afetados, o que motivou a instauração de processo administrativo pelo Departamento de Proteção e Defesa do Consumidor (DPDC), ainda antes da entrada em vigor da LGPD. Com base em revisão bibliográfica e análise documental, a pesquisa evidencia que o Facebook violou diversos princípios fundamentais da LGPD, tais como a finalidade, necessidade, transparência e segurança. A conduta da plataforma, ao permitir o acesso de terceiros aos dados de usuários e seus contatos sem supervisão efetiva, representa grave afronta aos direitos fundamentais à privacidade e à proteção dos dados pessoais. Além disso, observa-se a ausência de medidas preventivas e de notificação tempestiva aos usuários e às autoridades, o que intensifica a responsabilidade jurídica da empresa. A análise jurídica demonstra que a LGPD estabelece mecanismos eficazes de responsabilização civil, permitindo que o titular do dado pessoal lesado possa buscar reparação por danos morais e materiais, além da possibilidade de aplicação de sanções administrativas por parte da Autoridade Nacional de Proteção de Dados (ANPD). O caso em questão destaca a importância da responsabilização solidária entre os agentes de tratamento e a necessidade de maior controle sobre operadores externos. Também ressalta o papel da ANPD na fiscalização da conformidade e na promoção de uma cultura de proteção de dados no Brasil. Conclui-se que a responsabilização do Facebook é juridicamente fundamentada e socialmente necessária para garantir a efetividade da LGPD e proteger os titulares de dados em um ambiente digital cada vez mais vulnerável. A pesquisa reafirma a importância de políticas de governança de dados, consentimento legítimo e transparência como elementos centrais para a preservação da dignidade humana e da cidadania digital.

Palavras-chave: LGPD; responsabilidade civil; dados pessoais; plataformas digitais; Facebook; Cambridge Analytica.

ABSTRACT

This study aims to analyze the civil liability of digital platforms in cases of unauthorized sharing of personal data, under the General Data Protection Law (Law No. 13.709/18), using the Facebook–Cambridge Analytica scandal as a case study. Widely reported by international media, the case revealed that the social network allowed, through an external application, access to the data of up to 87 million users without their informed and specific consent. In Brazil, approximately 443,000 users were affected, which led to the opening of an administrative proceeding by the Consumer Protection Department (DPDC), even before the LGPD came into force. Based on a bibliographic review and documentary analysis, the research shows that Facebook violated several core principles of the LGPD, such as purpose limitation, necessity, transparency, and security. The platform's conduct, by allowing third-party access to user data and their contacts without effective oversight, constitutes a serious infringement of the fundamental rights to privacy and data protection. Moreover, the absence of preventive measures and prompt notification to users and authorities increases the company's legal liability. The legal analysis demonstrates that the LGPD establishes effective mechanisms for civil liability, enabling data subjects to seek compensation for moral and material damages, in addition to the imposition of administrative sanctions by the Brazilian National Data Protection Authority (ANPD). The case emphasizes the importance of joint liability among data processing agents and the need for stricter control over external operators. It also underscores the role of ANPD in monitoring compliance and fostering a culture of data protection in Brazil. It is concluded that Facebook's liability is legally justified and socially necessary to ensure the effectiveness of the LGPD and safeguard data subjects in an increasingly vulnerable digital environment. The study reaffirms the importance of data governance policies, legitimate consent, and transparency as central elements for preserving human dignity and digital citizenship.

Keywords: LGPD; civil liability; personal data; digital platforms; Facebook; Cambridge Analytica.

SUMÁRIO

1 INTRODUÇÃO.....	8
2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): FUNDAMENTOS E APLICAÇÃO.....	11
2.1 FUNDAMENTOS E PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS.....	12
2.2 ANTECEDENTES DA LGPD NO CONTEXTO LEGAL BRASILEIRO.....	16
2.3 APLICAÇÃO DA LGPD EM CRIMES CIBERNÉTICOS.....	20
3 RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO.....	25
3.1 CONCEITO E PRESSUPOSTOS DA RESPONSABILIDADE CIVIL.....	27
3.2 RESPONSABILIDADE OBJETIVA E SUBJETIVA NAS RELAÇÕES DIGITAIS.....	30
3.3 REPARAÇÃO DE DANOS MORAIS E MATERIAIS EM CASOS DE VAZAMENTO DE DADOS.....	34
4 O PAPEL DAS PLATAFORMAS DIGITAIS NA SEGURANÇA DOS DADOS PESSOAIS.....	37
4.1 DEVERES LEGAIS DAS PLATAFORMAS DIGITAIS PERANTE A LGPD.....	38
4.2 MEDIDAS DE SEGURANÇA E PREVENÇÃO DE INCIDENTES DE DADOS.....	41
4.3 CONSEQUÊNCIAS JURÍDICAS DO DESCUMPRIMENTO DA LGPD PELAS PLATAFORMAS.....	44
5 ESTUDO DE CASO: O COMPARTILHAMENTO INDEVIDO DE DADOS PELO FACEBOOK.....	48
5.1 CONTEXTUALIZAÇÃO DO INCIDENTE DE VAZAMENTO DE DADOS.....	48
5.2 A ATUAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) NO CASO.....	52
5.3 ANÁLISE JURÍDICA DA RESPONSABILIDADE DO FACEBOOK À LUZ DA LGPD.....	54
CONSIDERAÇÕES FINAIS.....	57
REFERENCIAS.....	60

1 INTRODUÇÃO

A era digital transformou profundamente as relações sociais, econômicas e jurídicas ao redor do mundo, especialmente no que se refere à forma como os dados pessoais são coletados, armazenados e utilizados por empresas e governos. Nesse cenário, a informação digital tornou-se um dos ativos mais valiosos da atualidade, sendo utilizada para fins comerciais, publicitários e até políticos. No entanto, o uso desenfreado desses dados gerou a necessidade de uma normatização jurídica capaz de garantir a proteção da privacidade e da intimidade dos indivíduos, culminando na criação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que entrou em vigor no Brasil em 2020 (MACIEL, 2020).

A promulgação da LGPD representa um marco histórico no ordenamento jurídico brasileiro, pois estabelece um conjunto de princípios, direitos e deveres que orientam o tratamento de dados pessoais no país. Inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a lei brasileira busca assegurar que os titulares dos dados tenham controle sobre suas informações e que os agentes de tratamento atuem com responsabilidade, transparência e segurança (SOUZA, 2018). Nesse contexto, o incidente de compartilhamento indevido de dados por plataformas digitais, como o caso do Facebook, levanta relevantes questões sobre a efetividade da legislação e os mecanismos de responsabilização civil das empresas envolvidas.

O caso do Facebook, amplamente divulgado pela mídia nacional e internacional, consistiu na exposição indevida de informações de milhões de usuários, o que gerou intensos debates sobre os limites do consentimento, a ausência de mecanismos preventivos de proteção de dados e as consequências jurídicas decorrentes da violação da privacidade. Segundo reportagem publicada pelo Techtudo (BARROS, 2011), a empresa admitiu que o botão "curtir" presente em diversos sites coletava dados dos usuários mesmo quando não estavam logados, repassando informações sem autorização expressa. Tal conduta configura, à luz da LGPD, uma falha no dever de garantir o tratamento adequado das informações pessoais.

A responsabilidade civil, nesse sentido, emerge como instrumento fundamental para coibir práticas lesivas e assegurar a reparação dos danos causados aos titulares de dados. De acordo com Patrícia P. Pinheiro (2021), a responsabilização dos controladores e operadores de dados deve observar critérios objetivos e subjetivos, a

depender do tipo de violação e da conduta adotada pelos agentes. A LGPD prevê a possibilidade de responsabilização objetiva, ou seja, independentemente da comprovação de culpa, quando houver violação a direitos decorrente de tratamento inadequado ou não autorizado de dados pessoais.

Para além da responsabilização jurídica, há também uma dimensão ética e social envolvida na proteção de dados pessoais. Como destaca MIRAGAIA e BELMUDES (2008), o Estado, que deveria atuar como garantidor dos direitos humanos, muitas vezes figura como principal violador desses direitos, especialmente no que diz respeito à privacidade e à vigilância em massa. Essa perspectiva é corroborada por casos como o de Edward Snowden, que revelou a espionagem global promovida pelos Estados Unidos, inclusive com a colaboração de grandes empresas de tecnologia (PORTAL G1, 2013; SIMON, 2014).

A crescente coleta e comercialização de dados por empresas privadas sem o conhecimento ou consentimento do usuário levanta sérias preocupações sobre a vulnerabilidade do cidadão no ambiente digital. Como alerta Saulo Luz (2012), os dados pessoais estão literalmente à venda, sendo acessados e negociados por empresas sem qualquer controle por parte dos titulares. Isso evidencia a fragilidade da proteção jurídica anterior à LGPD e a necessidade urgente de regulamentações mais eficazes para conter abusos.

Nesse cenário, o controle judicial tem se mostrado um importante mecanismo de contenção das práticas abusivas. Em decisão emblemática, a Justiça brasileira não poupou o Google em processo por venda indevida de dados pessoais, reforçando a tese de que empresas devem ser responsabilizadas por condutas que afrontam direitos fundamentais (CONVERGÊNCIA DIGITAL, 2015). Da mesma forma, o episódio envolvendo o aplicativo Secret evidenciou o conflito entre liberdade de expressão e proteção à privacidade, com a Justiça suspendendo decisão de remoção da plataforma após pedido do Google (GONZAGA, 2014).

A análise da responsabilidade civil no compartilhamento indevido de dados, portanto, deve considerar os fundamentos constitucionais que garantem a proteção da intimidade, da vida privada e da autodeterminação informativa. Conforme argumenta BARBOSA (2021), o direito à proteção de dados é uma manifestação do direito fundamental à privacidade, estando intrinsecamente ligado à dignidade da pessoa humana. Assim, qualquer violação desses direitos deve ensejar a devida responsabilização dos infratores, com vistas à reparação integral dos danos.

A responsabilização civil por danos causados em decorrência do uso indevido de dados pessoais requer a identificação de elementos essenciais, como a existência do dano, o nexo causal e a conduta do agente. Segundo Fernando José da Costa (2011), em crimes informáticos, o *locus delicti* assume contornos específicos, já que os atos muitas vezes são praticados em ambientes virtuais de difícil rastreamento. Tal desafio impõe aos operadores do Direito a necessidade de desenvolver novas formas de interpretação e atuação no campo da responsabilidade digital.

Além disso, o discurso jurídico não pode ignorar as transformações sociotécnicas que afetam a noção de privacidade na contemporaneidade. GONÇALVES (2018) defende que a punição estatal por violações no âmbito digital deve ser acompanhada por políticas públicas educativas e preventivas, visando não apenas a repressão, mas também a formação de uma cultura de respeito aos direitos digitais. Nesse sentido, a responsabilização civil deve ser entendida como parte de um sistema mais amplo de governança de dados.

A atuação estatal, no entanto, nem sempre é eficaz ou imparcial. O caso do delegado Protógenes Queiroz, demitido por uso indevido do cargo (CONJUR, 2015), ilustra como o poder público também pode falhar em garantir o respeito aos direitos fundamentais. Essa realidade aponta para a necessidade de fortalecimento institucional dos órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD), prevista na LGPD, com atribuições específicas para fiscalizar, orientar e aplicar sanções administrativas às empresas que descumprirem a lei.

O contexto brasileiro, portanto, demanda um olhar atento para os desafios e lacunas na aplicação da LGPD. Como destaca MENDES (2019), a lei precisa ser interpretada à luz dos princípios constitucionais e dos tratados internacionais dos quais o Brasil é signatário, de forma a garantir a máxima efetividade à proteção dos dados pessoais. Nesse sentido, é imprescindível que o Judiciário atue de forma firme e coerente na responsabilização das plataformas digitais que promovem o uso indevido dessas informações.

No caso específico do Facebook, observa-se uma clara violação aos princípios da finalidade, da necessidade e da transparência, previstos na LGPD. A coleta de dados por meio de cookies, sem o devido consentimento do usuário, configura conduta lesiva e passível de responsabilização civil. Como afirma MACIEL (2020), a conformidade com a legislação de proteção de dados exige mudanças estruturais nas práticas corporativas, com a implementação de medidas técnicas e administrativas eficazes.

A proteção de dados deve ser compreendida como uma extensão do próprio direito à cidadania. A exposição indevida de informações pode gerar danos materiais e morais significativos, afetando a reputação, a integridade psíquica e até a segurança física do indivíduo. Assim, o ordenamento jurídico brasileiro, ao estabelecer a responsabilidade civil por danos decorrentes do tratamento inadequado de dados, reafirma seu compromisso com a dignidade humana e com a construção de um ambiente digital mais justo e seguro.

Nesse sentido, o presente estudo propõe-se a analisar a responsabilidade civil no incidente de compartilhamento indevido de dados pessoais no caso do Facebook, à luz da LGPD, buscando compreender os fundamentos jurídicos, os limites da responsabilização e as implicações sociais dessa temática. A partir da análise doutrinária, legislativa e jurisprudencial, pretende-se contribuir para o debate sobre os caminhos possíveis para a efetiva proteção dos dados pessoais no Brasil.

2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): FUNDAMENTOS E APLICAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como uma resposta à crescente preocupação com o uso indiscriminado de dados pessoais por entes públicos e privados. Ela estabelece regras claras sobre a coleta, o armazenamento, o tratamento e o compartilhamento dessas informações, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. A LGPD representa um avanço significativo no ordenamento jurídico brasileiro, colocando o Brasil em sintonia com legislações internacionais, como o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), e trazendo segurança jurídica para as relações digitais.

O texto legal define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável, e dá tratamento especial aos chamados dados sensíveis, como aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, dados genéticos ou biométricos. A lei também traz o conceito de "titular dos dados", isto é, o indivíduo a quem os dados se referem, e estabelece os direitos desses titulares, tais como o direito à confirmação do tratamento, ao acesso aos dados, à correção, à portabilidade e à exclusão, salvo nos casos em que a conservação é

legalmente exigida. O foco da LGPD é conferir maior autonomia e controle ao cidadão sobre suas próprias informações.

Para garantir a aplicação efetiva da lei, a LGPD instituiu figuras jurídicas como o controlador e o operador de dados, responsáveis, respectivamente, por tomar decisões sobre o tratamento dos dados e por realizá-lo em nome do controlador. Ambos estão sujeitos a obrigações legais, como a necessidade de consentimento livre, informado e inequívoco do titular, a transparência no uso das informações e a adoção de medidas de segurança para prevenir acessos não autorizados, vazamentos e outras formas de uso indevido. A lei também determina a criação de um encarregado pelo tratamento de dados (o "DPO"), cuja função é atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Desta forma a LGPD prevê sanções administrativas para os casos de descumprimento de suas normas, que vão desde advertências até multas significativas e a publicização da infração. Além das sanções administrativas, a violação dos direitos do titular pode gerar responsabilidade civil por danos materiais ou morais. A aplicação da LGPD, portanto, exige não apenas o cumprimento técnico das exigências legais, mas também uma mudança cultural nas organizações, que devem priorizar a proteção da privacidade como valor central de sua atuação. Assim, a LGPD consolida um novo paradigma jurídico no Brasil, pautado pelo respeito à dignidade da pessoa humana no ambiente digital.

2.1 Fundamentos e princípios da proteção de dados pessoais

A proteção de dados pessoais emerge, no contexto jurídico contemporâneo, como um dos pilares essenciais para a garantia dos direitos fundamentais no ambiente digital. A promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), representou uma resposta normativa ao acelerado avanço tecnológico e à consequente vulnerabilidade dos indivíduos diante da coleta e tratamento indiscriminado de suas informações. Essa legislação estabelece um marco regulatório no Brasil, promovendo a defesa da dignidade da pessoa humana, da privacidade e da autodeterminação informativa como elementos centrais da proteção de dados (PINHEIRO, 2021).

A Constituição Federal de 1988 já reconhecia, ainda que implicitamente, a proteção de dados pessoais ao consagrar os direitos à intimidade, à vida privada e à imagem no artigo 5º, incisos X e XII. Contudo, foi apenas com a LGPD que tais garantias foram sistematizadas e operacionalizadas de forma concreta no ordenamento jurídico brasileiro. A norma consagrou princípios e fundamentos específicos que orientam a atuação de agentes públicos e privados no tratamento de dados pessoais, reforçando o papel do Estado na tutela dos direitos fundamentais, conforme sublinhado por Mendes (2019), ao tratar da construção conceitual da proteção de dados como um direito autônomo.

Entre os fundamentos elencados no artigo 2º da LGPD, destaca-se a necessidade de respeito à privacidade, o que implica o reconhecimento do titular de dados como sujeito de direitos e não apenas como objeto de interesses comerciais. Além disso, a autodeterminação informativa, ou seja, o direito do indivíduo de controlar as informações relativas à sua pessoa, é apontada como um dos pilares dessa nova era da proteção de dados. Mendes (2019) salienta que esse fundamento consolida a ideia de que os dados pessoais pertencem ao indivíduo, e não à empresa ou entidade que os coleta.

Conforme estabelecido no artigo 2º da Lei Geral de Proteção de Dados (LGPD), os fundamentos da proteção de dados pessoais são:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Outro fundamento relevante é o desenvolvimento econômico e tecnológico, que demonstra o esforço do legislador em compatibilizar a proteção de dados com a inovação. Nesse sentido, a LGPD não se propõe a frear o progresso tecnológico, mas sim a garantir que ele ocorra de maneira ética, segura e transparente. A obra de Maciel (2020) contribui para essa compreensão ao destacar que a proteção de dados deve ser

vista como um elemento de fortalecimento da confiança nas relações digitais, o que é benéfico para o ambiente de negócios e para a sociedade em geral.

O ordenamento jurídico brasileiro passa, portanto, a adotar uma abordagem principiológica para lidar com os desafios da sociedade da informação. Os princípios expressamente previstos no artigo 6º da LGPD estabelecem balizas interpretativas e normativas para a atuação dos agentes de tratamento. Dentre eles, o princípio da finalidade impõe que o tratamento de dados seja realizado para propósitos legítimos, específicos e informados ao titular, vedada a utilização posterior de forma incompatível com tais finalidades.

Na mesma linha, o princípio da adequação exige a compatibilidade do tratamento com as finalidades informadas, ao passo que o princípio da necessidade determina que apenas os dados estritamente necessários sejam tratados. Esses princípios atuam conjuntamente no sentido de evitar excessos e abusos, funcionando como filtros normativos indispensáveis à conformidade legal das operações com dados pessoais (BARBOSA, 2021).

O princípio do livre acesso garante ao titular a consulta facilitada sobre a forma e a duração do tratamento, bem como a integralidade de seus dados pessoais. Já o princípio da qualidade dos dados assegura que as informações tratadas sejam exatas, claras, relevantes e atualizadas. Essa diretriz está relacionada ao dever de diligência dos agentes de tratamento e reforça o caráter dinâmico da responsabilidade prevista na LGPD.

Outro princípio de destaque é o da transparência, que impõe ao controlador a obrigação de fornecer informações claras, precisas e facilmente acessíveis aos titulares. A transparência está diretamente conectada ao princípio da boa-fé, que permeia toda a atuação jurídica em matéria de proteção de dados. Como pontua Gonçalves (2018), a ausência de transparência na relação entre titulares e controladores contribui para a assimetria informacional, o que fragiliza a posição jurídica do cidadão no ambiente digital.

A segurança também figura como princípio basilar da LGPD, exigindo a adoção de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração e comunicação. Em consonância, o princípio da prevenção impõe uma postura proativa na mitigação de riscos, exigindo dos agentes de tratamento a adoção de boas práticas e políticas de governança em proteção de dados (MACIEL, 2020).

Por sua vez, o princípio da não discriminação veda o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos, assegurando a igualdade material nas relações digitais. Esse princípio ganha especial relevo quando se observa o uso de tecnologias baseadas em algoritmos e inteligência artificial, que podem reproduzir ou até amplificar preconceitos sociais, caso não sejam acompanhadas de mecanismos de supervisão e correção.

O princípio da responsabilização e prestação de contas encerra o rol do artigo 6º da LGPD, atribuindo aos agentes de tratamento o dever de demonstrar, de forma clara e objetiva, a adoção de medidas eficazes para o cumprimento das normas de proteção de dados. Trata-se de um princípio que reafirma a importância da governança, da cultura da conformidade e da accountability, conforme destacado por Souza (2018), ao tratar da influência do modelo europeu na formulação da LGPD brasileira.

Esses princípios atuam de forma integrada e interdependente, constituindo o núcleo normativo da LGPD e norteando sua aplicação tanto no âmbito privado quanto no setor público. A sua observância não se restringe a uma formalidade legal, mas se projeta como instrumento de efetividade dos direitos fundamentais no ciberespaço. Assim, a proteção de dados pessoais transcende o campo da mera regulação econômica, assumindo contornos constitucionais e sociais inegáveis.

É nesse cenário que a análise do caso Facebook, envolvendo o compartilhamento indevido de dados de usuários, adquire especial relevância. A empresa, ao permitir a exposição de informações pessoais sem o consentimento expresso dos titulares, viola frontalmente os princípios da finalidade, da necessidade e da transparência, configurando hipótese concreta de responsabilização civil, conforme será aprofundado nos capítulos seguintes (BARROS, 2011).

O incidente citado gerou ampla repercussão na mídia e reacendeu o debate sobre os limites éticos e jurídicos das plataformas digitais. A veiculação do ocorrido por veículos como o Techtudo e a análise crítica de especialistas em direito digital evidenciam a gravidade das consequências sociais e jurídicas decorrentes da violação da LGPD (CONVERGÊNCIA DIGITAL, 2015). Ao mesmo tempo, reforçam a importância dos princípios normativos da proteção de dados como instrumentos de controle democrático e proteção cidadã.

O fundamento da proteção de dados não reside apenas na prevenção de danos materiais, mas sobretudo na defesa da dignidade humana em sua dimensão informacional. Como lembra Miragaia e Belmudes (2008), o Estado, mesmo com o

dever de proteção, é muitas vezes o maior violador de direitos fundamentais, o que exige vigilância constante e mecanismos eficazes de responsabilização. Da mesma forma, empresas privadas que atuam como agentes de tratamento devem se comprometer com a observância rigorosa dos princípios da LGPD.

Portanto, é evidente que os fundamentos e princípios da proteção de dados pessoais não são meras abstrações jurídicas, mas sim dispositivos concretos de defesa da liberdade individual e da integridade moral dos cidadãos. Sua incorporação ao ordenamento jurídico brasileiro através da LGPD representa um avanço normativo relevante, mas que depende de aplicação efetiva e fiscalização adequada para alcançar seus objetivos. Nesse sentido, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e do Poder Judiciário será determinante para consolidar uma cultura de respeito à privacidade e à proteção de dados no Brasil.

Com base nessa estrutura normativa principiológica e à luz do caso Facebook, é possível avaliar de forma crítica e fundamentada os limites e possibilidades da responsabilidade civil decorrente do compartilhamento indevido de dados pessoais em plataformas digitais. Tal análise será aprofundada no próximo capítulo, tendo por norte a interpretação sistemática da LGPD e os preceitos do direito civil contemporâneo.

2.2 Antecedentes da LGPD no contexto legal brasileiro

A proteção de dados pessoais, embora consolidada juridicamente apenas recentemente por meio da Lei Geral de Proteção de Dados (LGPD), possui raízes legais profundas que precedem o próprio desenvolvimento da tecnologia digital. Muito antes da criação da LGPD, a preocupação com a privacidade do indivíduo já ocupava espaço nas legislações nacionais e internacionais. A Declaração Universal dos Direitos Humanos de 1948 foi um dos primeiros documentos a tratar dessa questão em âmbito global, afirmando em seu artigo 12 que "ninguém será sujeito a interferências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem a ataques à sua honra e reputação", o que estabelece um marco ético e jurídico sobre a inviolabilidade da privacidade humana (Declaração Universal dos Direitos Humanos, 1948).

Essa mesma linha de pensamento foi incorporada na Constituição Federal de 1988, que conferiu status de direito fundamental à intimidade e à vida privada. Os

incisos X, XI e XII do artigo 5º asseguram, respectivamente, a inviolabilidade da intimidade e da vida privada, a proteção do domicílio como asilo inviolável e o sigilo das comunicações, incluindo dados, exceto por ordem judicial em situações específicas (Brasil, 1988). Esses dispositivos deixam clara a preocupação do legislador com a proteção da esfera íntima do cidadão, consolidando um conjunto de garantias que seriam cada vez mais exigidas com o avanço das tecnologias.

No entanto, com o passar do tempo e com o surgimento de tecnologias que permitiram o tratamento massivo de dados pessoais — como internet, redes sociais e aplicativos — essas garantias passaram a se mostrar insuficientes. Como destacou Mulholland (2012, p. 3), o avanço tecnológico e a disseminação da internet facilitaram o acesso a dados sensíveis, tornando mais frequente e mais grave a violação da privacidade. Assim, passou-se a compreender que a privacidade não se limitava à proteção da vida íntima, mas englobava também o controle sobre as próprias informações pessoais.

Ainda nos anos 1990, começaram a surgir leis que buscavam lidar com esses novos desafios. O Código de Defesa do Consumidor de 1990 (Lei nº 8.078) foi uma das primeiras legislações brasileiras a reconhecer implicitamente a importância dos dados pessoais, ao assegurar o direito à informação adequada e clara sobre os diferentes produtos e serviços, bem como o direito à proteção contra práticas comerciais abusivas, o que abrange o uso indevido de dados (Brasil, 1990).

Posteriormente, a Lei nº 9.296/1996, que dispõe sobre a interceptação de comunicações telefônicas e telemáticas, estabeleceu que tais interceptações só poderiam ocorrer com autorização judicial, reforçando o princípio do sigilo das comunicações previsto na Constituição (Brasil, 1996). Nesse mesmo sentido, a Lei do Habeas Data (Lei nº 9.507/1997) foi outro avanço importante, pois garantiu aos cidadãos o direito de acessar informações pessoais armazenadas por entidades públicas e privadas, bem como de corrigi-las caso estivessem incorretas (Brasil, 1997).

O Código Civil de 2002 também incorporou dispositivos relevantes sobre o direito à privacidade. Seu artigo 21 afirma de maneira explícita que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2002). Trata-se de um reforço importante às garantias já previstas constitucionalmente, reconhecendo o valor da esfera privada como direito indisponível.

Com a crescente digitalização da sociedade brasileira, foi necessária uma legislação mais específica. Em 2012, a Lei nº 12.737, popularmente conhecida como Lei Carolina Dieckmann, tipificou crimes relacionados à invasão de dispositivos eletrônicos. A lei surgiu após o vazamento de fotos íntimas da atriz que deu nome à norma e serviu como um alerta sobre a fragilidade das informações digitais. A inclusão dos artigos 154-A e 154-B no Código Penal proporcionou uma resposta penal mais clara aos crimes cibernéticos (Brasil, 2012).

Antes dessa lei, a invasão de dispositivos era considerada apenas um ato preparatório, ou seja, não configurava crime em si. Com sua promulgação, passou-se a tratar como delito a ação de acessar dispositivos alheios sem autorização, seja para obtenção, adulteração ou destruição de dados, seja para a instalação de vulnerabilidades. Como consequência, a legislação brasileira passou a contar com um instrumento de proteção penal no ambiente virtual, o que representou um avanço no campo da segurança digital.

A promulgação da Lei nº 12.737/2012 foi um divisor de águas para o debate público sobre privacidade e segurança digital no Brasil. A repercussão midiática do caso Carolina Dieckmann sensibilizou a sociedade e reforçou a urgência de um arcabouço legal que fosse capaz de proteger o cidadão frente às novas ameaças digitais. A partir dali, a construção de uma cultura de proteção de dados começou a ganhar força no país, culminando no desenvolvimento de legislações mais abrangentes.

Em 2014, foi sancionado o Marco Civil da Internet (Lei nº 12.965), que passou a regular os direitos e deveres dos usuários e provedores de serviços de internet no Brasil. Em seu artigo 7º, a lei garante a inviolabilidade da intimidade e da vida privada dos usuários, bem como o sigilo do fluxo de comunicações online. Também exige consentimento expresso para o armazenamento e o uso de dados pessoais (Brasil, 2014).

Segundo Bonfati e Kolbe (2020, p. 66), a velocidade do avanço tecnológico impôs novos desafios ao Direito, obrigando os juristas a repensarem seus paradigmas tradicionais e a adaptarem a normatividade às exigências de um ambiente virtual dinâmico e muitas vezes transfronteiriço. É nesse contexto que o Marco Civil da Internet surge como um marco regulatório necessário e inovador.

O Marco Civil da Internet também previu o direito à exclusão definitiva dos dados após o término da relação entre o usuário e o provedor de serviços, garantindo que a permanência dessas informações nos bancos de dados não ocorra de forma indefinida. Além disso, impôs transparência na coleta, armazenamento e

compartilhamento de dados, promovendo maior controle por parte do usuário (Brasil, 2014).

Apesar de todos esses avanços, ainda se sentia a ausência de uma legislação que disciplinasse, de forma sistematizada, o tratamento de dados pessoais em todos os setores da economia e da administração pública. A crescente pressão social, somada a exigências internacionais de compliance, sobretudo oriundas da União Europeia, intensificaram o debate sobre a necessidade de uma lei geral de proteção de dados.

Nesse ínterim, observa-se que o direito à privacidade evoluiu do conceito tradicional de não interferência na vida privada para uma concepção mais ampla, que engloba o controle individual sobre os dados pessoais. Tal percepção é evidenciada por Mulholland (2012), ao afirmar que o indivíduo deve ter o direito de decidir como, quando e por quem suas informações podem ser utilizadas, o que é especialmente relevante diante da capacidade das tecnologias atuais de coletar, processar e compartilhar dados em larga escala.

A ausência de uma regulação geral sobre dados pessoais gerava insegurança jurídica tanto para cidadãos quanto para empresas, que se viam diante de lacunas legais ao tratar dados sensíveis. A LGPD, inspirada na General Data Protection Regulation (GDPR) da União Europeia, veio justamente para preencher esse vácuo legislativo e estabelecer regras claras para o tratamento de dados, inclusive prevendo sanções administrativas pelo descumprimento da norma.

Dessa forma, a LGPD representa a consolidação de um processo histórico e legislativo que teve início com garantias constitucionais e foi gradualmente sendo reforçado por normas infraconstitucionais específicas. Trata-se de um desdobramento natural e necessário diante da complexidade e dos riscos envolvidos na sociedade da informação.

Além disso, a promulgação da LGPD fortalece a soberania informacional dos cidadãos, permitindo que estes exerçam maior controle sobre os seus dados, inclusive com o direito de retificação, eliminação e portabilidade. Esse novo paradigma jurídico reforça a ideia de autodeterminação informativa, tão cara ao constitucionalismo contemporâneo.

Outro aspecto relevante é o impacto da LGPD na atuação das organizações públicas e privadas, que passaram a ter o dever de estruturar programas de governança de dados, capacitar equipes e adotar medidas técnicas de segurança da informação. Esse

movimento também incentivou a profissionalização de áreas como compliance digital e segurança cibernética.

Portanto, os antecedentes da LGPD demonstram que a proteção de dados pessoais no Brasil não surgiu do nada, mas sim como resposta a um conjunto de fatores históricos, jurídicos e sociais que, ao longo das décadas, foram moldando a consciência coletiva sobre a importância da privacidade como um direito fundamental. A LGPD é, assim, um capítulo atual de uma longa jornada legislativa que começou com os ideais de 1948 e se concretizou com os desafios do século XXI.

2.3 Aplicação da LGPD em crimes cibernéticos

Os crimes cibernéticos representam uma nova fronteira da criminalidade, surgindo como reflexo direto da intensificação do uso da tecnologia e da internet no cotidiano. Trata-se de práticas ilícitas que utilizam dispositivos eletrônicos, redes digitais ou sistemas de computação para a execução de crimes. Segundo Silva (2022), tais delitos podem ocorrer tanto contra sistemas informáticos quanto utilizando esses sistemas como meio para atingir a vítima. A amplitude dos crimes cibernéticos abrange desde ataques a bancos de dados até fraudes, invasões, disseminação de conteúdo ilegal e ataques à honra, sendo facilitados pelo anonimato e pela difícil rastreabilidade dos autores na rede mundial de computadores.

Entre os crimes cibernéticos mais recorrentes no Brasil estão o furto de identidade virtual, fraudes eletrônicas, estelionato, disseminação de malwares, cyberbullying e pornografia infantil. As redes sociais, como Facebook, Instagram e WhatsApp, tornaram-se palco constante de práticas criminosas que, muitas vezes, não são imediatamente percebidas como tais. De acordo com Beuren e Almeida (2012), o crescimento do uso das redes digitais como canal de comunicação e transações comerciais elevou o risco de violações de dados pessoais e crimes contra usuários desavisados, especialmente aqueles com pouca instrução digital.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, foi criada para regulamentar o tratamento de dados pessoais no Brasil, garantindo maior segurança, transparência e controle aos titulares dos dados. Sua importância no combate aos crimes cibernéticos está relacionada à responsabilização de empresas e instituições quanto ao uso indevido ou inseguro das informações pessoais.

Nicolini (2021) destaca que a LGPD não apenas busca prevenir a utilização ilícita dos dados, mas também promove a reparação civil quando esses dados são comprometidos em incidentes como ataques hackers ou vazamentos.

Os crimes cibernéticos podem ser classificados como próprios ou impróprios. Os próprios são aqueles que só podem ocorrer no ambiente digital, como a invasão de dispositivo informático e a disseminação de malwares. Já os impróprios consistem em crimes comuns adaptados para a internet, como calúnia, ameaça e estelionato. Darós (2020) explica que essa classificação é essencial para o enquadramento jurídico correto dos crimes, considerando as nuances da prática criminosa no ambiente virtual. Essa distinção também afeta diretamente a responsabilização dos autores e a aplicabilidade das normas protetivas, como a LGPD.

Ameaça virtual é um dos crimes cibernéticos mais comuns e pode ocorrer por meio de mensagens em redes sociais, e-mails ou aplicativos de mensagem instantânea. A LGPD não trata diretamente da ameaça, mas quando há vazamento ou uso indevido de dados para ameaçar alguém, a lei pode ser aplicada de forma subsidiária. Segundo Araújo (2016), a proteção da integridade dos dados está intimamente ligada à integridade da própria pessoa, sendo possível aplicar a LGPD em casos onde informações pessoais são utilizadas como instrumento de coação ou violência psicológica.

A participação em suicídio e a indução a esse ato pela internet têm se tornado uma preocupação crescente, especialmente com a ascensão de comunidades virtuais que incentivam esse tipo de comportamento. A LGPD pode ser relevante nesses casos quando plataformas digitais falham em proteger os dados dos usuários, expondo-os a conteúdos que incentivam a autodestruição. A autora Juliana Ferreira da Silva enfatiza que há uma zona de corresponsabilidade entre os gestores das plataformas e a sociedade civil, uma vez que o tratamento irresponsável de dados sensíveis pode potencializar vulnerabilidades emocionais.

A incitação e a apologia ao crime, quando realizadas no ambiente digital, se tornam ainda mais perigosas pela velocidade com que se espalham e pelo alcance das redes sociais. A LGPD, nesses casos, atua de maneira indireta, principalmente quando há coleta e uso de dados para segmentar públicos vulneráveis a esse tipo de conteúdo. Roque (2021) observa que a governança de dados nas plataformas precisa se alinhar com princípios éticos e legais que dificultem o uso da tecnologia para promover comportamentos criminosos.

A violação de direitos autorais na internet também é um crime cibernético que afeta diversos setores, principalmente os culturais e acadêmicos. O compartilhamento ilegal de obras protegidas por direito autoral, como livros, músicas e filmes, pode envolver o tratamento indevido de dados dos autores ou das plataformas onde o conteúdo foi veiculado. Nicolini (2021) salienta que, ao proteger o dado pessoal do autor, a LGPD contribui para coibir a disseminação de obras sem autorização, fortalecendo o respeito à propriedade intelectual.

A falsidade ideológica, quando praticada por meio de documentos digitais ou perfis falsos, tem como base o uso de dados inverídicos ou manipulados. A LGPD, ao impor regras para coleta e validação de dados pessoais, contribui significativamente para a prevenção desse tipo de crime. Conforme Silva (2022), a criação de perfis com informações falsas pode causar danos tanto à pessoa representada quanto à integridade dos sistemas digitais, sendo fundamental o uso ético e legal dos dados no meio virtual.

A falsa identidade, um crime cibernético muito presente nas redes sociais, ocorre quando alguém se passa por outra pessoa, muitas vezes com o objetivo de enganar terceiros ou cometer fraudes. A LGPD oferece respaldo jurídico ao titular dos dados ao permitir a solicitação de exclusão de perfis falsos e o direito de retificação de informações. Beuren e Almeida (2012) destacam que, embora a LGPD não criminalize diretamente essas ações, ela oferece mecanismos de defesa que fortalecem a posição da vítima frente ao provedor de internet e às plataformas digitais.

Os crimes contra a honra — calúnia, difamação e injúria — são amplamente cometidos em ambientes digitais. A rapidez e a falta de filtros nas redes sociais contribuem para a propagação de ofensas, com impacto devastador na vida da vítima. A LGPD pode ser aplicada nesses casos quando as plataformas se omitem quanto à remoção de conteúdo ofensivo que envolva dados pessoais. Segundo Martins (2020), há uma linha tênue entre liberdade de expressão e o respeito à dignidade humana, e a LGPD atua como instrumento de equilíbrio nesse contexto.

O racismo virtual é um crime gravíssimo e frequentemente ocorre em comentários, publicações ou mensagens privadas. A LGPD tem papel importante na identificação e responsabilização de autores desses crimes, já que permite rastrear e proteger dados da vítima e do autor, desde que cumpridos os trâmites legais. Darós (2020) aponta que a proteção de dados não deve ser usada como escudo para o anonimato criminoso, mas sim como instrumento de justiça e dignidade humana, especialmente para minorias historicamente vulnerabilizadas.

A intrusão informática, ou hacking, envolve o acesso não autorizado a sistemas e dispositivos. Esse é um crime cibernético próprio, e a LGPD é diretamente aplicável, já que trata da segurança da informação como princípio essencial. Coelho et al. (2018) explicam que as organizações que não implementam medidas de segurança adequadas podem ser responsabilizadas civilmente quando há vazamento de dados causados por invasões.

O furto de identidade virtual é uma das formas mais danosas de crime cibernético, já que envolve a utilização de dados pessoais de terceiros para realizar ações fraudulentas. A LGPD protege o titular desses dados e obriga as empresas a comunicar qualquer vazamento, permitindo a adoção de medidas imediatas. De acordo com Roque (2021), a lei estabelece bases legais claras para o uso de dados, e seu descumprimento pode configurar negligência ou até conivência com fraudes.

A inserção de malwares, programas maliciosos que afetam o funcionamento de sistemas e coletam dados de forma ilícita, representa uma grave violação da privacidade digital. A LGPD estabelece obrigações de segurança da informação que, se descumpridas, tornam a instituição responsável pelo dano sofrido. Nicolini (2021) ressalta que, mesmo que o ataque venha de fora, a falta de um plano de resposta a incidentes pode implicar sanções legais à empresa envolvida.

A engenharia social, técnica usada para manipular usuários e obter dados sensíveis, depende da coleta prévia de informações pessoais. A LGPD atua preventivamente ao exigir consentimento explícito para uso de dados e medidas de transparência. Silva (2022) observa que, em muitos casos, a violação começa com o uso indevido de dados coletados sem conhecimento do titular, o que reforça a necessidade de fiscalização ativa.

A pornografia infantil é um dos crimes mais graves cometidos no ambiente virtual. A LGPD pode colaborar com as investigações ao regular o armazenamento e a rastreabilidade de dados em plataformas digitais, facilitando a atuação das autoridades. Juliana Ferreira (2023) afirma que a lei pode funcionar como instrumento de proteção da infância ao impedir o uso indiscriminado de imagens e dados de crianças e adolescentes.

O cyberbullying, prática de intimidação e humilhação online, é comum entre jovens e adolescentes. A LGPD pode ser aplicada ao exigir que as plataformas digitais removam conteúdo ofensivo que envolva dados pessoais e responsabilizem os autores.

Beuren e Almeida (2012) defendem que, ao proteger os dados dos usuários, a LGPD também protege sua dignidade e integridade emocional.

A xenofobia digital, como manifestação de preconceito contra estrangeiros, também pode ser denunciada e tratada com apoio da LGPD. A coleta de dados sensíveis, como origem nacional, pode ser considerada discriminatória se usada para hostilizar pessoas em plataformas digitais. Araújo (2016) destaca que a lei garante direitos fundamentais mesmo no ambiente virtual.

A vingança pornográfica, ou “porn revenge”, é o ato de divulgar imagens íntimas sem consentimento. A LGPD tem papel decisivo nesses casos, pois estabelece o direito ao apagamento de dados pessoais e à reparação por danos morais. Martins (2020) observa que o consentimento para uso de imagens é revogável a qualquer momento, e sua violação representa infração grave.

O furto mediante fraude, crime onde o agente se aproveita de dados para enganar a vítima, está entre os delitos mais praticados na internet. A LGPD exige que instituições financeiras protejam os dados de seus clientes com rigor técnico, e o descumprimento dessa exigência pode gerar indenizações. Darós (2020) afirma que, além da esfera criminal, há reflexos importantes na esfera cível com base na LGPD.

O estelionato virtual, que ocorre geralmente via e-mails e sites falsos, é um crime impróprio adaptado ao meio digital. A coleta ilícita de dados para fins fraudulentos é expressamente combatida pela LGPD. Roque (2021) reforça que a transparência no uso de dados é uma das chaves para evitar esse tipo de crime, e as empresas devem investir em campanhas educativas e protocolos de verificação.

A ciberextorsão envolve a ameaça de exposição de dados pessoais em troca de dinheiro ou favores. Nesses casos, a LGPD oferece suporte à vítima ao exigir que o controlador dos dados tome medidas imediatas para estancar o vazamento e coopere com as autoridades. Nicolini (2021) explica que a responsabilização é solidária, quando se comprova negligência da parte controladora dos dados.

O typosquatting é uma prática onde sites com nomes semelhantes aos de grandes marcas são criados para enganar usuários. A LGPD pode ser aplicada quando há coleta de dados de usuários por meio desses sites falsos, responsabilizando quem os criou ou hospedou. Beuren e Almeida (2012) reforçam que a rastreabilidade de IPs e a exigência de segurança são essenciais para prevenir essas práticas.

O stalking, ou perseguição digital, é uma prática que ganhou destaque jurídico com a criminalização em 2021. A LGPD atua ao proteger os dados de localização,

contatos e hábitos da vítima, que frequentemente são utilizados pelo agressor. Martins (2020) afirma que a regulamentação do tratamento de dados reduz a margem para abusos e facilita a punição dos responsáveis.

A interface entre a LGPD e os crimes cibernéticos é essencialmente protetiva. A lei não substitui o Código Penal, mas oferece suporte à vítima e orientações às empresas e plataformas sobre o que deve ou não ser feito com dados pessoais. Ao garantir transparência, segurança e direitos dos titulares, a LGPD se consolida como instrumento estratégico no combate à criminalidade digital, segundo Nicolini (2021).

Por fim, é evidente que a LGPD representa um marco na luta contra os crimes cibernéticos. Ela não resolve todas as questões, mas oferece um arcabouço jurídico que fortalece os direitos dos cidadãos em um ambiente digital cada vez mais complexo. A colaboração entre legislação penal, civil e de proteção de dados é essencial para um combate eficaz e ético da criminalidade virtual. Como afirmam Darós (2020) e Roque (2021), o futuro da segurança digital passa necessariamente pela educação, regulação e responsabilização.

3 RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO

O capítulo segundo capítulo tem como foco a análise do regime jurídico aplicável à responsabilização por danos decorrentes da violação de dados pessoais no ordenamento brasileiro. Inicialmente, é importante compreender que a responsabilidade civil é um dos pilares do sistema jurídico, pois garante a reparação dos danos causados por condutas ilícitas ou abusivas. Quando se trata da proteção de dados, essa responsabilidade ganha contornos específicos, dada a natureza sensível das informações pessoais e o impacto significativo que o uso indevido desses dados pode gerar na vida dos titulares.

Neste contexto, a Lei Geral de Proteção de Dados (LGPD) surge como marco regulatório essencial para disciplinar o tratamento de dados no Brasil. A legislação estabelece princípios e fundamentos que devem nortear o uso de informações pessoais, além de prever mecanismos de responsabilização para os agentes de tratamento – controladores e operadores – que desrespeitarem as normas legais. A LGPD trouxe inovações importantes ao prever não apenas a reparação de danos materiais, mas

também de danos morais, consolidando o direito à privacidade como um direito fundamental no país.

A responsabilização, conforme delineado pela LGPD, pode ser tanto subjetiva quanto objetiva, a depender do caso concreto. Em algumas situações, exige-se a comprovação de culpa ou dolo por parte do agente, enquanto em outras a mera ocorrência do dano e do nexo causal é suficiente para a responsabilização. O capítulo também aborda a responsabilidade solidária entre controlador e operador, reforçando a ideia de que todos os envolvidos no tratamento de dados devem agir com diligência, transparência e segurança.

Outro ponto essencial do capítulo é a análise da aplicação da responsabilidade civil em cenários concretos de incidentes de segurança da informação, como vazamentos de dados e ataques cibernéticos. A partir desses exemplos, busca-se compreender como o judiciário tem interpretado os dispositivos legais e quais os critérios adotados para a fixação de indenizações. Ressalta-se, ainda, a importância da adoção de boas práticas de governança de dados pelas empresas, como forma de mitigar riscos e demonstrar conformidade com a legislação.

Desta forma, o capítulo evidencia o papel do Poder Judiciário e da Autoridade Nacional de Proteção de Dados (ANPD) na efetividade das normas de proteção de dados, destacando a importância da fiscalização e da aplicação de sanções como instrumentos de coerção e prevenção. A responsabilização civil, nesse sentido, funciona não apenas como mecanismo de reparação, mas também como meio de educar e orientar os agentes econômicos sobre a necessidade de respeito aos direitos fundamentais dos titulares de dados

3.1 Conceito e pressupostos da responsabilidade civil

A responsabilidade civil é um dos pilares fundamentais do ordenamento jurídico brasileiro e se expressa pela obrigação de reparar o dano causado a outrem em decorrência de uma conduta ilícita ou culposa. Segundo Venosa (2020), a responsabilidade civil possui o objetivo primário de recompor o patrimônio do lesado, retornando-o ao estado anterior ao ato lesivo. Essa reparação pode ser de ordem material ou moral, sendo que, no contexto contemporâneo, os danos imateriais, como aqueles

causados por ataques cibernéticos ou uso indevido de dados pessoais, têm recebido atenção especial da doutrina e da jurisprudência.

Para que haja a configuração da responsabilidade civil, é necessário o preenchimento de três pressupostos essenciais: a conduta (ação ou omissão), o dano e o nexo de causalidade entre ambos. Em determinadas situações, exige-se ainda a presença da culpa do agente, conforme pontua Gonçalves (2022), caracterizando a responsabilidade subjetiva. Contudo, há hipóteses em que a responsabilização independe da verificação de culpa, tratando-se da responsabilidade objetiva, cuja base é o risco da atividade desempenhada.

A conduta, como primeiro pressuposto, é entendida como o comportamento humano voluntário, que pode se manifestar como ação ou omissão. Maria Helena Diniz (2021) enfatiza que a conduta é o ponto de partida para a configuração da responsabilidade, pois sem ela não há como falar em dano juridicamente relevante. No contexto digital, por exemplo, o compartilhamento não autorizado de dados pessoais constitui uma conduta ativa, enquanto a ausência de medidas de segurança adequadas configura uma omissão relevante.

O segundo pressuposto, o dano, refere-se à lesão a um bem jurídico tutelado, podendo se manifestar sob a forma de prejuízo material, moral ou até mesmo existencial. Segundo Tartuce (2021), o dano é o elemento central da responsabilidade civil e sua demonstração é imprescindível para a procedência da pretensão reparatória. O autor ressalta ainda que o dano deve ser certo, atual e juridicamente relevante, não bastando a mera possibilidade ou conjectura de prejuízo.

O nexo de causalidade, terceiro elemento da responsabilidade, é a ligação entre a conduta e o dano. De acordo com Gonçalves (2022), o nexo causal deve ser direto e imediato, excluindo-se situações em que o dano resulta de causas alheias à conduta do agente, como caso fortuito ou força maior. No campo da proteção de dados, essa conexão pode se tornar complexa, dada a multiplicidade de agentes envolvidos no tratamento e a dificuldade de identificar a origem exata do vazamento ou uso indevido da informação.

Além desses três pressupostos, a culpa é analisada quando se trata da responsabilidade subjetiva. Conforme Venosa (2020), a culpa se subdivide em negligência, imprudência ou imperícia e deve ser demonstrada pelo lesado. Entretanto, quando a legislação estabelece responsabilidade objetiva – como no caso das relações

de consumo e na LGPD –, a análise da culpa é dispensada, bastando a demonstração do dano e do nexo causal.

A responsabilidade objetiva encontra respaldo no parágrafo único do art. 927 do Código Civil, que estabelece que haverá obrigação de reparar o dano, independentemente de culpa, nos casos em que a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. Diniz (2021) argumenta que esse dispositivo consagra a teoria do risco, segundo a qual quem auferir lucros com determinada atividade deve arcar com os riscos dela decorrentes.

Nesse sentido, a LGPD também consagra a responsabilidade objetiva dos agentes de tratamento de dados, especialmente quando há falha na segurança da informação. A Lei 13.709/2018 prevê, em seu art. 42, que o controlador ou operador que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo a outrem, é obrigado a repará-lo. Tartuce (2021) observa que essa previsão legal fortalece o regime protetivo ao titular dos dados e impõe um padrão mais elevado de diligência aos agentes.

Outro aspecto relevante no contexto da responsabilidade civil moderna é o dano moral. Maria Helena Diniz (2021) enfatiza que o dano moral decorre da ofensa a atributos da personalidade, como a honra, a imagem e a privacidade. Nas situações envolvendo dados pessoais, especialmente quando ocorre vazamento ou exposição indevida, o dano moral pode ser presumido, considerando a gravidade da ofensa ao direito à privacidade do titular.

A jurisprudência brasileira tem reconhecido a aplicação da responsabilidade civil em casos envolvendo ilícitos digitais e violação de dados. Gonçalves (2022) relata que a consolidação do entendimento jurisprudencial tem reforçado a importância da proteção da esfera íntima do cidadão e a função pedagógica da responsabilidade civil. Os tribunais têm responsabilizado provedores, plataformas digitais e empresas por falhas na proteção de dados de seus usuários.

Além disso, a responsabilidade civil pode ser solidária quando há mais de um agente envolvido na prática do ato danoso. Conforme Venosa (2020), a solidariedade decorre da indivisibilidade do dano e da necessidade de assegurar a reparação integral ao lesado. No âmbito da proteção de dados, essa solidariedade é aplicada entre controlador e operador quando ambos contribuem para o evento danoso, como preceitua o art. 42, §1º da LGPD.

Tartuce (2021) destaca ainda que a reparação do dano deve ser integral, ou seja, capaz de reconstituir o patrimônio do lesado da forma mais completa possível. Isso inclui a indenização por lucros cessantes, danos emergentes e, quando cabível, danos morais. A função da responsabilidade civil, portanto, não é apenas compensatória, mas também preventiva e punitiva, desestimulando a prática de condutas lesivas.

O dever de indenizar também impõe aos agentes a obrigação de prevenir o dano. Diniz (2021) pontua que a responsabilidade civil moderna está cada vez mais voltada à ideia de prevenção, de modo que as empresas devem adotar políticas e mecanismos que minimizem os riscos de danos, como o compliance digital e a governança de dados pessoais. A LGPD, nesse sentido, funciona como um instrumento preventivo ao prever sanções e incentivos à adoção de boas práticas.

A responsabilidade civil também é impactada pelas novas tecnologias e pela dinâmica da internet. Gonçalves (2022) ressalta que os desafios atuais envolvem não apenas o reconhecimento do dano e de seus autores, mas também a execução da reparação, especialmente quando os agentes estão fora da jurisdição nacional. Isso exige uma atualização constante da doutrina e da jurisprudência, bem como a cooperação internacional.

A responsabilização civil também desempenha papel importante na garantia dos direitos fundamentais. Venosa (2020) afirma que a responsabilidade civil tem função constitucional, pois assegura o respeito à dignidade da pessoa humana e aos direitos da personalidade. No caso da violação de dados pessoais, trata-se de uma afronta direta à privacidade e ao controle sobre a própria informação, elementos centrais da autonomia individual.

Por fim, a evolução da responsabilidade civil exige uma compreensão interdisciplinar, que dialogue com áreas como o direito digital, a proteção de dados, a psicologia e a sociologia. Maria Helena Diniz (2021) reforça que o direito deve se adaptar às transformações sociais e tecnológicas, oferecendo respostas adequadas aos novos conflitos que surgem no ambiente virtual. O respeito à privacidade e o tratamento ético dos dados são questões que ultrapassam a esfera jurídica e refletem valores sociais fundamentais.

Assim, o estudo do conceito e dos pressupostos da responsabilidade civil, à luz da legislação atual e da realidade digital, permite compreender a importância desse instituto na proteção dos direitos dos indivíduos e na regulação das condutas sociais. A responsabilidade civil não é apenas um mecanismo de compensação, mas também um

instrumento de justiça, que visa equilibrar as relações sociais e assegurar o respeito aos direitos fundamentais, especialmente em tempos de sociedade da informação.

3.2 Responsabilidade objetiva e subjetiva nas relações digitais

A rápida evolução tecnológica dos últimos anos provocou transformações profundas na forma como as pessoas se comunicam, trabalham, consomem e interagem socialmente. A ascensão da internet e das tecnologias digitais criou um ambiente dinâmico, com novas oportunidades, mas também com riscos significativos, especialmente no que tange à proteção de dados pessoais, segurança da informação e integridade das relações jurídicas no espaço virtual. Nesse cenário, o Direito precisou adaptar-se com celeridade, criando mecanismos capazes de acompanhar o ritmo da inovação e assegurar os direitos fundamentais dos usuários. Conforme Gonçalves (2022), o mundo digital exigiu uma reinterpretação de institutos clássicos, como a responsabilidade civil, à luz dos novos desafios do ambiente eletrônico.

O Direito, historicamente considerado um sistema conservador em sua evolução, foi pressionado a responder aos danos causados por atos praticados por meio eletrônico, muitas vezes anônimos ou de difícil rastreabilidade. A responsabilização por esses atos passou a ser discutida não apenas com base nos critérios tradicionais da culpa, mas também por meio da responsabilização objetiva, baseada no risco e na teoria da responsabilidade sem culpa. Segundo Venosa (2020), essa adaptação se faz necessária diante da dificuldade prática de se comprovar a intenção ou negligência em contextos digitais, onde a identificação do agente é, muitas vezes, complexa ou impossível.

As relações digitais caracterizam-se por sua informalidade, transnacionalidade e imediatismo, o que desafia os padrões tradicionais de responsabilização. Com o aumento de fraudes, golpes virtuais, vazamentos de dados, uso indevido de informações pessoais, entre outros ilícitos, tornou-se evidente a necessidade de proteger os usuários e consumidores com base em modelos de responsabilidade mais eficientes. Para Tartuce (2021), esse contexto favoreceu a adoção da responsabilidade objetiva, especialmente nos casos em que há desequilíbrio entre as partes, como nas relações de consumo eletrônicas.

A responsabilidade subjetiva, baseada na demonstração de culpa – entendida como negligência, imprudência ou imperícia –, continua a ser aplicada em muitas

situações, principalmente quando o dano é causado por indivíduos e não por empresas ou plataformas. Contudo, essa modalidade de responsabilização apresenta limitações no ambiente digital. De acordo com Maria Helena Diniz (2021), a subjetividade da culpa, aliada à volatilidade das provas digitais, pode dificultar ou inviabilizar a reparação do dano, prejudicando a eficácia do sistema jurídico.

Diante disso, a responsabilidade objetiva surge como um instrumento jurídico eficaz para garantir a tutela dos direitos dos usuários na internet, principalmente quando o agente causador do dano desenvolve atividade de risco ou atua em desequilíbrio de forças com o lesado. O Código de Defesa do Consumidor (Lei nº 8.078/1990), por exemplo, já previa essa modalidade de responsabilização, e foi amplamente incorporado nas relações digitais. Gonçalves (2022) lembra que, no ambiente virtual, o consumidor é especialmente vulnerável e, por isso, merece proteção reforçada.

A LGPD (Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018) também adota a responsabilidade objetiva em diversos dispositivos, especialmente em relação ao controlador e operador de dados. Segundo Tartuce (2021), o art. 42 da referida lei deixa claro que, em caso de danos patrimoniais, morais, individuais ou coletivos, o agente de tratamento de dados é obrigado a indenizar, independentemente de culpa, bastando que se comprove a relação causal entre a falha e o dano sofrido pelo titular dos dados.

A responsabilidade objetiva, nesse contexto, baseia-se na teoria do risco da atividade. Se determinada empresa ou organização se beneficia economicamente do tratamento de dados, ela deve assumir os riscos relacionados à segurança e confidencialidade dessas informações. Como explica Venosa (2020), quem auferir vantagens com determinada atividade deve suportar os ônus dela decorrentes. Isso significa que a empresa que lucra com o uso de dados pessoais tem o dever de garantir sua proteção.

Apesar da adoção da responsabilidade objetiva, a responsabilidade subjetiva não foi abolida do ordenamento, sendo ainda aplicada em diversos contextos. A diferença reside na necessidade, ou não, de demonstrar a culpa do agente. Maria Helena Diniz (2021) destaca que, em casos onde o autor do dano é um usuário comum da internet, que compartilha conteúdos ofensivos ou pratica cyberbullying, a culpa deve ser demonstrada para que se configure a obrigação de indenizar.

Por outro lado, quando se trata de grandes plataformas digitais, provedores de serviços ou empresas de e-commerce, a responsabilidade tende a ser objetiva,

especialmente quando se verifica a falha no dever de segurança, informação ou transparência. Conforme Gonçalves (2022), o dever de cautela é intensificado para esses agentes econômicos, que devem adotar todas as medidas possíveis para evitar o dano, sob pena de serem responsabilizados objetivamente.

Um exemplo prático é o vazamento de dados pessoais decorrente de falha em sistemas de segurança digital. Nesse caso, mesmo que não haja dolo ou culpa direta da empresa, a mera ocorrência do vazamento, desde que gere dano ao titular, já é suficiente para a caracterização da responsabilidade civil objetiva. Tartuce (2021) observa que, nessa hipótese, o controlador deverá demonstrar que não agiu com negligência, sendo este o chamado "ônus da prova invertido", típico das relações de consumo e agora também aplicado à proteção de dados.

Importante destacar que a LGPD também prevê excludentes de responsabilidade, como nos casos em que o dano decorre de culpa exclusiva do titular dos dados ou de terceiros. Contudo, a empresa deverá comprovar tais excludentes, sendo sua obrigação demonstrar que adotou todas as medidas necessárias à proteção dos dados. Venosa (2020) afirma que o modelo atual impõe um padrão elevado de diligência aos agentes de tratamento, o que reforça o caráter preventivo da responsabilidade objetiva.

O mesmo se aplica às plataformas digitais, como redes sociais e marketplaces, que, embora não sejam os autores diretos de conteúdos lesivos, podem ser responsabilizadas se não removerem, em tempo razoável, informações ofensivas após notificação. Maria Helena Diniz (2021) argumenta que essa responsabilidade decorre do dever de vigilância, sobretudo quando há reincidência de condutas ou omissão reiterada por parte da plataforma.

No ambiente digital, os danos morais são frequentemente mais difíceis de quantificar, mas não menos graves. A ofensa à honra, à imagem e à privacidade tem consequências profundas, especialmente em casos de exposição pública nas redes sociais. Gonçalves (2022) defende que, nesses casos, a reparação deve considerar não apenas os prejuízos concretos, mas também os efeitos psicológicos e sociais causados à vítima.

A responsabilidade objetiva, ao dispensar a prova da culpa, facilita o acesso à justiça e assegura maior proteção às vítimas de crimes ou infrações digitais. Entretanto, ela também impõe maior rigor e investimento às empresas, que devem adotar políticas eficazes de proteção de dados, segurança da informação e compliance digital. Segundo

Tartuce (2021), a adoção de medidas preventivas não elimina a responsabilidade, mas pode atenuar suas consequências ou demonstrar boa-fé do agente.

Ainda no campo da responsabilidade subjetiva, sua aplicação é mais comum em casos de relações interpessoais no meio digital, como insultos em redes sociais, compartilhamento de conteúdo íntimo sem consentimento ou práticas de stalking. Nesses casos, a análise do dolo ou culpa é fundamental para que o juiz possa avaliar a gravidade da conduta e fixar a indenização adequada. Venosa (2020) observa que, nesses cenários, a individualização da conduta do ofensor é essencial.

O desafio, portanto, está em estabelecer parâmetros claros para aplicação de cada modelo de responsabilidade. Enquanto a responsabilidade objetiva busca garantir eficácia e proteção imediata, a responsabilidade subjetiva ainda preserva princípios fundamentais, como a presunção de inocência e a necessidade de comprovação da culpa. Maria Helena Diniz (2021) propõe um modelo híbrido, onde os dois sistemas convivam de maneira harmônica, dependendo da natureza da relação jurídica e do perfil dos envolvidos.

A jurisprudência brasileira tem evoluído no sentido de reconhecer a responsabilidade objetiva das plataformas digitais em diversas situações. Em decisões recentes, os tribunais têm condenado empresas por falhas na moderação de conteúdo, vazamento de dados, fraudes em compras online, entre outros, mesmo sem prova direta de culpa. Conforme Gonçalves (2022), isso reforça a função social da responsabilidade civil como instrumento de equilíbrio nas relações digitais.

O ordenamento jurídico brasileiro, assim, caminha para consolidar uma estrutura de responsabilidade civil robusta e adaptada ao mundo digital. A aplicação da responsabilidade objetiva em relações marcadas pela assimetria de poder contribui para a proteção da parte mais fraca, como o consumidor ou o titular de dados. Tartuce (2021) destaca que essa tendência atende não apenas a princípios jurídicos, mas também às expectativas sociais de justiça e proteção.

Contudo, é importante que essa responsabilização não seja abusiva ou desproporcional, sob pena de desestimular a inovação e a liberdade na internet. Venosa (2020) adverte que o direito deve equilibrar proteção e liberdade, garantindo reparação adequada sem inviabilizar a atividade econômica digital. O papel do Judiciário, nesse sentido, é fundamental para interpretar as normas de forma sensata e ponderada.

A distinção entre responsabilidade objetiva e subjetiva nas relações digitais deve ser feita a partir da análise do contexto específico de cada situação. A tendência é a

ampliação da responsabilidade objetiva, especialmente para agentes econômicos que exploram dados e serviços digitais. Já a responsabilidade subjetiva continua relevante nas interações pessoais e na responsabilização individual por condutas ilícitas.

Dessa forma, o Direito brasileiro avança no enfrentamento dos desafios do ambiente digital, adaptando-se por meio da ampliação do escopo da responsabilidade objetiva e da manutenção da responsabilidade subjetiva em contextos apropriados. O equilíbrio entre esses dois modelos é essencial para garantir segurança jurídica, proteção eficaz e preservação da liberdade na internet, como bem concluem os autores citados.

3.3 Reparação de danos morais e materiais em casos de vazamento de dados

A reparação de danos decorrentes do vazamento de dados pessoais em ambientes digitais é um dos pilares fundamentais da Lei Geral de Proteção de Dados (LGPD), consagrada pela Lei nº 13.709/2018. A legislação estabelece, no artigo 42, que o controlador ou operador que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo. A responsabilização pode se dar com base na responsabilidade subjetiva, caso seja necessário comprovar culpa, ou objetiva, nos casos em que houver infração legal ou contratual claramente demonstrada. Conforme destaca MACIEL (2020), a LGPD inaugura um sistema que não apenas tutela o direito à privacidade, mas estabelece mecanismos concretos de responsabilização e compensação em favor do titular lesado.

O entendimento jurídico brasileiro tem evoluído no sentido de reconhecer o dano moral como presumido em casos de vazamento de dados sensíveis, especialmente quando envolve a exposição de informações de cunho íntimo, como orientação sexual, histórico médico, dados bancários e localização geográfica. Conforme aponta PINHEIRO (2021), a exposição indevida desses dados compromete não apenas a privacidade, mas também a dignidade do indivíduo, justificando a indenização por danos morais mesmo quando não há demonstração de prejuízo econômico direto. Essa lógica encontra eco no entendimento de FERNANDES (2021), que assinala que a violação do sigilo de dados configura afronta a um direito fundamental, o que torna legítima a reparação automática pelo simples descumprimento da norma protetiva.

A jurisprudência nacional já tem trilhado esse caminho, reconhecendo o dano moral como presumível em diversas decisões. O caso do Facebook, investigado por

compartilhamento indevido de dados de milhões de usuários com empresas terceiras, é paradigmático nesse sentido. A empresa foi acusada de violar a confiança dos usuários ao permitir que dados fossem utilizados sem o devido consentimento, o que gerou debates sobre a responsabilidade objetiva da plataforma. Como observa BARBOSA (2021), o caso evidencia o poder das big techs e a assimetria informacional entre as plataformas e os titulares de dados, o que reforça a necessidade de sanções exemplares e reparações compatíveis com a gravidade da ofensa.

A doutrina de BARRETO (2020) reforça que a reparação deve atender a um critério de proporcionalidade e efetividade. Isto é, deve-se levar em conta a extensão do dano, a capacidade econômica do agente causador e a necessidade de desestimular práticas negligentes por parte das empresas. Nesse contexto, a indenização por dano moral cumpre também uma função pedagógica e preventiva, pois incentiva o fortalecimento das políticas de segurança da informação e o cumprimento dos princípios da boa-fé, da finalidade e da necessidade no tratamento dos dados pessoais.

Além dos danos morais, é perfeitamente possível a cumulação com danos materiais, conforme previsto pelo Código Civil (Lei nº 10.406/2002), notadamente em seu artigo 927. Os danos materiais referem-se aos prejuízos financeiros diretamente mensuráveis que o titular sofre, como uso indevido de dados bancários, realização de transações fraudulentas ou negativação indevida do nome em cadastros de inadimplentes. Segundo ALVES (2020), nos crimes digitais, há um desafio adicional na quantificação do dano, especialmente em razão da multiplicidade de agentes e da volatilidade das evidências digitais, o que demanda um aprimoramento técnico e jurídico contínuo.

A LGPD também prevê a figura da responsabilidade solidária entre o controlador e o operador de dados, o que amplia o escopo de responsabilização e protege o titular. A responsabilização solidária assegura que qualquer um dos agentes envolvidos na cadeia de tratamento de dados possa ser acionado judicialmente para reparar o dano, ficando a cargo destes o direito de regresso. De acordo com BOMFATI e KOLBE JUNIOR (2020), essa estrutura jurídica é necessária para combater a impunidade digital e garantir a efetividade da reparação, principalmente em ecossistemas complexos como os das redes sociais, onde os dados trafegam entre múltiplas instâncias.

BOITEUX (2010) chama atenção para a necessidade de um tratamento jurídico internacional coordenado para que a reparação de danos em vazamentos de dados seja

eficaz em um mundo hiperconectado. Isso porque, em casos como o do Facebook, a empresa atua em diversas jurisdições, o que dificulta a responsabilização uniforme. Ainda que a LGPD tenha inspiração em normas como o GDPR europeu, o alcance prático da reparação depende da existência de cooperação internacional, tratados e mecanismos eficazes de cumprimento extraterritorial de decisões judiciais.

O impacto da reparação também se estende à esfera coletiva. A LGPD, em seu artigo 52, admite sanções administrativas e ações civis públicas movidas por entidades de defesa do consumidor ou do Ministério Público. Nesses casos, a indenização pode ter caráter coletivo, voltado à compensação de danos sociais decorrentes da quebra massiva de privacidade. Conforme analisa MENDES e BRANCO (2019), a tutela coletiva dos direitos fundamentais digitais é uma evolução necessária do Direito Constitucional, pois reconhece o impacto societal dos vazamentos de dados em escala.

A complexidade das relações digitais demanda uma atuação efetiva do Judiciário, que deve ser capacitado para lidar com provas eletrônicas, responsabilidade múltipla e critérios técnicos de segurança da informação. DA COSTA (2011) defende a criação de varas especializadas em crimes digitais e vazamentos de dados, a fim de agilizar a análise das provas e garantir maior eficácia na reparação dos danos. Essa especialização também permitiria decisões mais técnicas e alinhadas com a evolução dos meios tecnológicos utilizados tanto na coleta quanto no uso indevido dos dados.

No aspecto probatório, os desafios são amplos. A doutrina de BITENCOURT (2021) observa que o ônus da prova pode ser invertido, especialmente quando há evidente hipossuficiência do consumidor frente às grandes plataformas digitais. Essa inversão, prevista no Código de Defesa do Consumidor e recepcionada pela LGPD, busca equilibrar a relação jurídica e garantir que o lesado não seja duplamente penalizado: pelo vazamento e pela dificuldade de comprovação. Assim, a reparação de danos em vazamentos de dados se consolida também como mecanismo de equidade.

A atuação das plataformas digitais, como o Facebook, diante das denúncias de vazamento, é também elemento relevante para a definição da extensão da responsabilidade e da indenização. Segundo BARROS (2011), a resposta inicial da empresa foi de negação da gravidade do problema, o que agravou a percepção pública de omissão e negligência. Tal comportamento é reprovado pela LGPD, que exige comunicação imediata ao titular e à ANPD em caso de incidentes de segurança, sendo o descumprimento desse dever mais um elemento passível de aumentar o valor da reparação.

A função reparatória do direito civil, em se tratando de dados pessoais, vai além da compensação monetária. Ela deve alcançar também a restauração da confiança do cidadão no sistema digital. Como destaca GONÇALVES (2018), a proteção dos dados é um pilar essencial para a consolidação da cidadania digital, e a falha nesse aspecto compromete não apenas o titular, mas a legitimidade das instituições. Por isso, a reparação adequada é um imperativo jurídico, ético e social no enfrentamento dos abusos cometidos no ciberespaço.

Por fim, vale considerar que a reparação dos danos morais e materiais em casos de vazamento de dados deve ser pensada como parte de uma política pública de proteção digital, articulada com educação digital, regulação tecnológica e vigilância democrática. NASCIMENTO (2020) sublinha que a Constituição Federal de 1988 consagra a proteção à intimidade e à privacidade como cláusulas pétreas, o que reforça o dever do Estado e dos particulares de assegurar um ambiente digital seguro. Nesse sentido, a reparação civil é apenas um dos instrumentos para garantir que o uso da tecnologia respeite os direitos fundamentais do cidadão.

4 O PAPEL DAS PLATAFORMAS DIGITAIS NA SEGURANÇA DOS DADOS PESSOAIS

A crescente dependência das plataformas digitais para comunicação, consumo, entretenimento e relações sociais impõe uma responsabilidade cada vez maior sobre essas empresas no que tange à segurança dos dados pessoais. Com o avanço das tecnologias de big data e a monetização de informações pessoais, plataformas como Facebook, Google e outras se tornaram não apenas depositárias de dados sensíveis, mas também agentes com poder significativo sobre a vida privada dos usuários. Como argumenta Maciel (2020), esse cenário exige um comprometimento concreto das plataformas com os princípios da transparência, finalidade e segurança previstos na Lei Geral de Proteção de Dados (Lei nº 13.709/18). A atuação dessas empresas, porém, nem sempre reflete a diligência esperada, como ficou evidente no caso do Facebook, cuja falha em impedir o uso indevido de informações de milhões de usuários foi amplamente noticiada (Barros, 2011).

A LGPD, ao atribuir obrigações tanto ao controlador quanto ao operador de dados, torna as plataformas digitais diretamente responsáveis pela adoção de medidas técnicas e administrativas capazes de proteger os dados sob sua custódia. Isso inclui não

apenas o tratamento adequado de dados, mas também a comunicação imediata de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, conforme previsto no artigo 48 da referida lei. Fernandes (2021) destaca que o papel das plataformas não deve ser apenas reativo, mas preventivo, exigindo políticas internas robustas, treinamento de equipes, auditorias periódicas e investimentos contínuos em segurança cibernética. Contudo, como observa Boiteux (2010), o modelo de negócio dessas empresas muitas vezes entra em conflito com a proteção da privacidade, pois a coleta massiva de dados alimenta seus algoritmos e potencializa sua lucratividade, criando um dilema ético e jurídico que desafia o ordenamento vigente.

Diante desse contexto, torna-se essencial repensar a governança de dados nas plataformas digitais e a responsabilidade que essas corporações assumem perante os usuários e a sociedade. Segundo Barreto e Brasil (2016), a segurança da informação deve ser tratada como um dever institucional, não uma faculdade mercadológica. Quando empresas falham em adotar práticas mínimas de proteção, não apenas infringem a LGPD, mas violam direitos fundamentais consagrados na Constituição Federal de 1988, como a intimidade, a vida privada e a dignidade da pessoa humana (Nascimento, 2020). Portanto, o papel das plataformas digitais na segurança de dados é mais do que uma questão técnica; trata-se de um compromisso jurídico, social e democrático com o respeito aos direitos dos titulares e com a integridade das relações digitais.

4.1 Deveres legais das plataformas digitais perante a LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi instituída como um marco regulatório fundamental para a proteção da privacidade e segurança da informação no Brasil. A partir dela, plataformas digitais — que atuam como controladoras e/ou operadoras de dados — passam a ter deveres legais rigorosos no que tange à coleta, armazenamento, tratamento, compartilhamento e exclusão de dados pessoais. De acordo com o artigo 6º da LGPD, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização devem orientar toda e qualquer atividade de tratamento de dados realizada por essas plataformas.

O dever de obter consentimento claro e informado do titular dos dados é uma das obrigações centrais impostas às plataformas digitais, conforme o artigo 7º da LGPD.

O consentimento deve ser livre, informado e inequívoco, e pode ser revogado a qualquer momento pelo titular, o que impõe um dever contínuo de gestão de consentimentos válidos. Como destaca Maciel (2020), muitas plataformas, como o Facebook, historicamente operaram com termos de uso genéricos e políticas de privacidade opacas, práticas que se tornaram inaceitáveis à luz da nova legislação.

Além disso, o artigo 9º da LGPD reforça o dever de transparência quanto ao uso de dados, exigindo das plataformas a disponibilização de informações claras e acessíveis sobre os critérios e procedimentos utilizados para tratamento automatizado, especialmente aqueles que afetam os interesses dos usuários, como a construção de perfis comportamentais ou decisões automatizadas. Fernandes (2021) ressalta que essa obrigação representa um avanço significativo na garantia de direitos informacionais, especialmente frente ao uso intensivo de algoritmos e inteligência artificial pelas big techs.

Outro dever relevante é o da segurança da informação. Nos termos do artigo 46 da LGPD, os agentes de tratamento de dados — incluindo as plataformas digitais — devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Boiteux (2010) aponta que, sem medidas eficazes de segurança, todo o sistema de proteção de dados fica fragilizado, pois não há controle efetivo sobre o risco de exposição indevida.

O artigo 48 da LGPD obriga os controladores a comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados, em prazo razoável, a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. A omissão dessa comunicação, como ocorreu em diversos escândalos envolvendo o Facebook (Barros, 2011), pode ser interpretada como agravante da responsabilidade civil e administrativa da plataforma, aumentando a extensão das sanções aplicáveis.

O dever de garantir os direitos dos titulares é ainda reforçado no artigo 18, que enumera prerrogativas como o acesso, correção, anonimização, portabilidade, eliminação e informação sobre o uso de dados. Barreto e Brasil (2016) argumentam que as plataformas devem manter canais eficientes de atendimento aos usuários e sistemas que permitam a gestão autônoma das informações por parte dos titulares, sob pena de violação direta da LGPD.

Outro ponto crítico diz respeito à base legal utilizada para o tratamento de dados. Conforme o artigo 7º da LGPD, o tratamento só pode ocorrer nas hipóteses autorizadas por lei, como o consentimento, cumprimento de obrigação legal, execução de políticas públicas, realização de estudos por órgão de pesquisa, execução de contrato, exercício regular de direitos, proteção da vida ou da saúde, tutela do crédito e legítimo interesse. Callegari (2019) destaca que muitas plataformas se escoram na base do "legítimo interesse", o que exige uma justificativa robusta e proporcional que deve ser avaliada pela ANPD e pelo Judiciário em caso de controvérsias.

No campo da responsabilização, a LGPD prevê no artigo 42 que o controlador ou operador que, em razão do tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, fica obrigado a repará-lo. Trata-se de uma responsabilidade que pode ser objetiva, quando houver violação de dever legal, ou subjetiva, nos casos que demandem comprovação de culpa. Maciel (2020) enfatiza que essa responsabilização amplia significativamente os riscos jurídicos para as plataformas, incentivando práticas mais seguras e transparentes.

Há, ainda, o dever de manutenção de registros das operações de tratamento de dados, como previsto no artigo 37 da LGPD, especialmente para agentes de tratamento de grande porte. Esses registros devem ser disponibilizados à ANPD mediante solicitação e servem como meio de auditoria e verificação do cumprimento das obrigações legais. Segundo Barreto (2020), essa exigência estimula o desenvolvimento de políticas internas de governança e compliance digital, que devem ser parte integrante da cultura organizacional das plataformas.

A designação de um encarregado pelo tratamento de dados pessoais, conforme estabelece o artigo 41, também é obrigatória. Esse profissional, conhecido como Data Protection Officer (DPO), deve atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Fernandes (2021) salienta que a ausência de um DPO capacitado compromete a implementação eficaz da LGPD e expõe a empresa a riscos legais significativos.

Com a vigência da LGPD, a atuação da ANPD como órgão fiscalizador se torna crucial. O artigo 55-J da LGPD confere à Autoridade Nacional competências como fiscalizar e aplicar sanções administrativas, orientar os agentes de tratamento, promover estudos e fomentar a educação em proteção de dados. Mendes e Branco (2019) observam que, para que a LGPD seja efetiva, é necessário que a ANPD tenha autonomia

técnica e recursos suficientes para exercer seu papel de forma independente e combativa.

As plataformas digitais também devem se submeter ao regime de sanções administrativas previsto no artigo 52 da LGPD, que incluem advertência, multa simples ou diária, publicização da infração, bloqueio ou eliminação dos dados pessoais relacionados à infração, suspensão parcial do funcionamento do banco de dados e até proibição parcial ou total do exercício das atividades relacionadas ao tratamento. Souza (2020) argumenta que a severidade das sanções é um elemento-chave para coibir práticas abusivas e assegurar a seriedade da conformidade legal.

Importante destacar que os deveres legais das plataformas não se esgotam na legislação nacional. A atuação dessas empresas em múltiplos países exige a observância de normativas internacionais, como o GDPR europeu. Como analisa Souza, Luíza (2018), a convergência normativa é benéfica para os titulares de dados, pois amplia a proteção e a previsibilidade jurídica no tratamento de informações pessoais transfronteiriças.

Vale ainda ressaltar que o cumprimento da LGPD pelas plataformas digitais deve ser encarado não como mero ônus jurídico, mas como parte integrante da responsabilidade social corporativa e da ética empresarial na era digital. Mendes (2019) sustenta que a proteção de dados é um direito fundamental que deve ser respeitado em todas as esferas de atuação empresarial, sendo a conformidade legal apenas o ponto de partida para uma cultura mais ampla de respeito à dignidade da pessoa humana na sociedade da informação.

4.2 Medidas de segurança e prevenção de incidentes de dados

A proteção de dados pessoais em ambientes digitais requer a adoção de medidas preventivas e corretivas que envolvam não apenas tecnologias sofisticadas, mas também políticas de governança da informação. A Lei Geral de Proteção de Dados (LGPD), especialmente em seu artigo 46, impõe aos agentes de tratamento — notadamente as plataformas digitais — o dever de adotar medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados, de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Segundo Fernandes (2021), a segurança da informação, nesse contexto, deve ser compreendida

como um compromisso contínuo e multifacetado, envolvendo aspectos técnicos, organizacionais, jurídicos e éticos.

Entre as medidas técnicas mais recomendadas pela doutrina estão o uso de criptografia, autenticação multifatorial, pseudonimização, controle de acesso, backups regulares e auditorias de sistemas. Maciel (2020) destaca que a escolha dessas ferramentas deve se basear em critérios de proporcionalidade e adequação, levando em conta a natureza dos dados tratados, os riscos envolvidos e a estrutura tecnológica disponível. A aplicação indiscriminada de tecnologias sem análise de impacto pode resultar em falhas operacionais e em uma falsa sensação de segurança.

As medidas administrativas são igualmente importantes e dizem respeito à criação de políticas internas de privacidade, códigos de conduta, treinamentos periódicos para os colaboradores, canais de comunicação com os titulares dos dados e nomeação de um encarregado pelo tratamento de dados (DPO). De acordo com Barreto (2020), essas medidas contribuem para a consolidação de uma cultura organizacional orientada à proteção de dados, o que é fundamental para mitigar os riscos de incidentes de segurança e garantir a conformidade com a LGPD.

A prevenção de incidentes também exige a realização periódica de relatórios de impacto à proteção de dados pessoais (RIPDs), conforme previsto no artigo 38 da LGPD. Esses relatórios devem identificar os riscos associados ao tratamento de dados e propor soluções de mitigação, funcionando como instrumentos preventivos fundamentais. Boiteux (2010) ressalta que o relatório de impacto é uma ferramenta jurídica e técnica essencial para antecipar vulnerabilidades e aprimorar a governança de dados, especialmente em empresas de grande porte que operam com tecnologias sensíveis.

A capacitação dos profissionais envolvidos no tratamento de dados é outro aspecto crucial. Segundo Bomfati e Kolbe Junior (2020), o fator humano ainda é a principal origem de falhas de segurança, seja por negligência, imperícia ou desconhecimento das normas e boas práticas. Dessa forma, o investimento em formação contínua sobre proteção de dados, cibersegurança e legislação aplicável não deve ser tratado como custo, mas como investimento estratégico para a redução de passivos jurídicos e danos reputacionais.

A atuação coordenada com fornecedores e terceiros também merece atenção. A LGPD estabelece que operadores de dados (prestadores de serviço contratados pelas plataformas) devem atuar conforme as instruções do controlador e estão sujeitos à

responsabilização solidária em caso de danos. Fernandes (2021) observa que contratos com cláusulas específicas sobre segurança da informação, auditoria e conformidade com a LGPD são indispensáveis para assegurar a cadeia de proteção dos dados e evitar “elos fracos” na rede de tratamento.

Um aspecto relevante no contexto de segurança é a existência de planos de resposta a incidentes. Tais planos devem prever procedimentos para a contenção, investigação, correção e comunicação de falhas de segurança. A Cartilha de Segurança para Internet do CERT.br (2023) recomenda que esses planos sejam atualizados com regularidade e testados em simulações para garantir sua eficácia. Como observa Callegari (2019), a resposta rápida e coordenada a incidentes pode minimizar danos, preservar provas digitais e demonstrar boa-fé perante autoridades fiscalizadoras e titulares afetados.

A obrigação de notificação de incidentes, disposta no artigo 48 da LGPD, exige que as plataformas informem à ANPD e aos titulares, em prazo razoável, qualquer evento que possa acarretar risco ou dano relevante. Essa medida visa garantir a transparência e permitir que os titulares adotem providências para mitigar os efeitos do vazamento, como troca de senhas ou contestação de movimentações financeiras. Segundo Pinheiro (2021), a demora ou omissão na notificação pode ser interpretada como agravante da infração e levar à aplicação de sanções mais severas.

O princípio da prevenção, previsto no artigo 6º, inciso VIII da LGPD, reforça a necessidade de antecipação e neutralização de riscos antes que eles se concretizem. Nascimento (2020) argumenta que a prevenção deve ser pensada como política pública e como parte integrante da responsabilidade social das plataformas digitais. Em um ambiente de riscos complexos e sofisticados, como o ciberespaço, não basta reagir após o dano: é preciso estruturar o sistema de proteção de forma proativa e resiliente.

Desta forma, a efetividade das medidas de segurança depende de fiscalização contínua por parte da Autoridade Nacional de Proteção de Dados (ANPD), além da atuação vigilante da sociedade civil e do Ministério Público. Mendes e Branco (2019) defendem que a proteção de dados deve ser incorporada à cultura jurídica nacional como um direito fundamental interligado à dignidade humana e à cidadania digital. Nesse sentido, as medidas de segurança e prevenção de incidentes não são apenas exigências técnicas da LGPD, mas instrumentos de fortalecimento democrático e promoção da confiança no ambiente digital.

4.3 Consequências jurídicas do descumprimento da LGPD pelas plataformas

O descumprimento da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) pelas plataformas digitais acarreta uma série de consequências jurídicas que podem ser de natureza civil, administrativa e, em alguns casos, até penal. A LGPD estabelece um marco normativo robusto que obriga os agentes de tratamento, incluindo grandes corporações tecnológicas, a respeitar os direitos dos titulares de dados e a adotar medidas eficazes de segurança da informação. Quando essas obrigações são ignoradas ou violadas, a legislação prevê uma série de sanções e responsabilizações que visam proteger a integridade e a privacidade dos usuários.

No campo civil, as plataformas digitais podem ser responsabilizadas pela reparação de danos causados aos titulares, nos termos do artigo 42 da LGPD. A responsabilidade poderá ser objetiva, isto é, independentemente da existência de culpa, quando houver violação da norma legal. Segundo Maciel (2020), isso representa uma inovação importante no direito brasileiro, pois desloca o foco da intenção do agente para os efeitos concretos do tratamento indevido de dados, promovendo maior proteção ao consumidor digital. Essa reparação pode incluir tanto danos morais quanto materiais, conforme também previsto no Código Civil (Lei nº 10.406/2002), em seu artigo 927.

O dano moral é amplamente reconhecido em casos de vazamento de dados, mesmo quando não há prejuízo econômico imediato. A jurisprudência tem adotado a tese do dano *in re ipsa*, ou seja, presume-se o abalo moral diante da violação da privacidade, especialmente quando envolvem dados sensíveis ou sigilosos. Pinheiro (2021) e Fernandes (2021) apontam que a jurisprudência vem consolidando essa perspectiva, reconhecendo que o simples fato de expor dados pessoais já configura ofensa à dignidade da pessoa humana, passível de reparação pecuniária.

A responsabilidade solidária entre os agentes de tratamento também é uma consequência importante prevista no artigo 42, §1º da LGPD. Plataformas digitais que contratam terceiros para operar dados — como empresas de publicidade ou serviços de armazenamento — podem ser responsabilizadas conjuntamente pelos danos causados. Segundo Bomfati e Kolbe Junior (2020), essa medida busca garantir que o titular do dado tenha acesso à reparação sem que precise apurar previamente a culpa individual de cada envolvido, fortalecendo o princípio da efetividade do direito à privacidade.

Do ponto de vista administrativo, o artigo 52 da LGPD prevê uma série de sanções que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD). Essas sanções incluem: advertência; multa simples de até 2% do faturamento da pessoa jurídica no Brasil (limitada a R\$ 50 milhões por infração); multa diária; publicização da infração; bloqueio dos dados pessoais a que se refere a infração; eliminação dos dados pessoais; suspensão parcial do funcionamento do banco de dados; e até a proibição parcial ou total do exercício da atividade de tratamento de dados.

A aplicação dessas sanções observa critérios como a gravidade e a natureza da infração, os direitos pessoais afetados, a boa-fé do infrator, a reincidência e o grau de dano. Barreto (2020) ressalta que as sanções administrativas são fundamentais para criar um ambiente de conformidade e dissuadir práticas negligentes ou dolosas no tratamento de dados. Ele destaca que a ANPD, ao exercer seu poder sancionador, deve também atuar de forma orientadora, promovendo a cultura da proteção de dados no país.

É importante observar que, além da LGPD, outras normas podem ser aplicadas cumulativamente em casos de violação, como o Código de Defesa do Consumidor (Lei nº 8.078/1990), especialmente quando o usuário é tratado como consumidor e os dados são utilizados para fins comerciais. Barreto e Brasil (2016) defendem a aplicação do CDC em conjunto com a LGPD para ampliar o espectro de proteção, garantindo acesso facilitado ao Judiciário, inversão do ônus da prova e responsabilização objetiva dos fornecedores de serviços digitais.

As consequências penais também podem surgir, especialmente quando o tratamento indevido de dados se dá de forma fraudulenta ou com intenção criminosa. A Lei nº 12.737/2012 (Lei Carolina Dieckmann), que alterou o Código Penal Brasileiro, tipifica condutas como invasão de dispositivos informáticos e divulgação indevida de dados eletrônicos. Segundo Bitencourt (2021), há uma interseção clara entre a LGPD e o Direito Penal, sobretudo quando os vazamentos de dados são resultado de ciberataques, extorsões ou engenharia social praticada com dolo.

A publicidade da infração, prevista no artigo 52, inciso III da LGPD, pode gerar danos reputacionais severos para a plataforma infratora. A obrigatoriedade de tornar pública a infração visa tanto à reparação simbólica quanto à função pedagógica e preventiva da sanção. Gonçalves (2018) sustenta que a perda de credibilidade e a fuga de usuários são consequências comerciais inevitáveis para empresas que demonstram fragilidade na proteção de dados, o que reforça a importância da conformidade como diferencial competitivo.

Em casos de infrações reiteradas ou de grande escala, a ANPD pode, inclusive, suspender o funcionamento da plataforma no Brasil, como já ocorreu com aplicativos como o Secret, conforme noticiado por Gonzaga (2014). Essa medida extrema é justificada pela necessidade de garantir a ordem pública, a moralidade e a segurança informacional dos cidadãos brasileiros, e demonstra o poder regulador conferido à Autoridade Nacional pela LGPD.

O dever de notificação de incidentes, previsto no artigo 48 da LGPD, caso descumprido, constitui infração autônoma que pode agravar a responsabilidade da plataforma. A omissão ou demora na comunicação à ANPD e aos titulares prejudicados pode ser entendida como má-fé ou tentativa de ocultar os danos, gerando penalidades mais severas. Conforme lembra Callegari (2019), a transparência na gestão de crises é um elemento central da governança digital moderna e sua ausência compromete não apenas a conformidade legal, mas a confiança do mercado e da sociedade.

A inação da empresa após a ocorrência de um incidente de segurança também é juridicamente relevante. Se a plataforma não adotar medidas imediatas para mitigar os danos e proteger os dados remanescentes, poderá responder por agravamento do dano, o que, conforme entendimento doutrinário de Mendes e Branco (2019), pode elevar o valor das indenizações e reforçar a caracterização da culpa.

Em termos processuais, a LGPD permite que os titulares de dados lesados ingressem individualmente ou coletivamente com ações judiciais para reparação de danos. O Ministério Público, a Defensoria Pública e entidades civis também podem propor ações civis públicas, nos moldes da Lei nº 7.347/1985. A atuação coletiva é especialmente importante quando os dados de milhares ou milhões de usuários são expostos, como ocorreu no caso do Facebook, analisado por Barros (2011).

Outro ponto relevante é que o descumprimento da LGPD pode ser considerado uma violação a direitos fundamentais previstos na Constituição Federal de 1988, como o direito à intimidade, à vida privada e à proteção da honra (art. 5º, incisos X e XII). Nascimento (2020) defende que o uso indevido de dados deve ser combatido com a mesma seriedade com que se enfrentam outras formas de violação de direitos humanos, pois a proteção dos dados é parte essencial da dignidade humana na sociedade digital.

A depender do caso concreto, também poderá haver responsabilização por enriquecimento ilícito, se a plataforma lucrar de forma indevida com dados coletados ilegalmente. A doutrina de Souza (2020) considera que esse tipo de

responsabilização tem função não apenas reparatória, mas também dissuasiva, impedindo que empresas se beneficiem economicamente de práticas ilícitas.

As consequências jurídicas não se restringem ao âmbito interno. Quando o descumprimento da LGPD afeta cidadãos estrangeiros ou viola tratados internacionais de proteção de dados, pode haver repercussões internacionais, inclusive com sanções aplicadas por entidades reguladoras de outros países, como a Comissão Europeia, nos casos em que a empresa também opere sob a égide do GDPR. Souza, Luíza (2018) aponta que a harmonização entre legislações é necessária para garantir proteção global e prevenir que as big techs explorem lacunas normativas entre os países.

Portanto, o descumprimento da LGPD pelas plataformas digitais não deve ser compreendido como uma infração isolada ou meramente formal. Trata-se de uma violação estrutural, com implicações diretas nos direitos fundamentais dos cidadãos, na estabilidade regulatória e no funcionamento da democracia digital. Como conclui Mendes (2019), a responsabilidade dessas empresas transcende o aspecto comercial: elas são guardiãs da privacidade e da liberdade informacional em uma sociedade hiperconectada, e devem agir com diligência compatível com esse papel.

5 ESTUDO DE CASO: O COMPARTILHAMENTO INDEVIDO DE DADOS PELO FACEBOOK

5.1 Contextualização do incidente de vazamento de dados

O escândalo envolvendo o Facebook e a Cambridge Analytica representou um divisor de águas no debate global sobre proteção de dados pessoais, evidenciando a fragilidade da privacidade dos usuários em plataformas digitais e o uso indevido de suas informações para fins políticos. A coleta massiva e não autorizada de dados de até 87 milhões de usuários – entre eles, 443 mil brasileiros – por meio do aplicativo “This Is Your Digital Life” revelou falhas sistêmicas no modelo de governança da plataforma e suscitou ampla discussão sobre os limites do consentimento digital. Segundo reportagens da *BBC News* (2018) e do *New York Times* (2018), os dados coletados foram utilizados para elaborar estratégias políticas de microdirecionamento, afetando diretamente campanhas eleitorais em diversos países, como Estados Unidos, Reino Unido e possivelmente Brasil e Índia.

O caso veio à tona após denúncias do ex-funcionário da Cambridge Analytica, Christopher Wylie, que revelou como o aplicativo desenvolvia perfis psicológicos dos usuários com base em suas interações sociais, curtidas, publicações e informações demográficas. O escândalo foi amplamente documentado em obras como o documentário “The Great Hack”, da Netflix, que retratou os bastidores da manipulação de informações e a atuação agressiva da consultoria britânica na exploração dos dados para fins eleitorais. As revelações levaram ao movimento global #DeleteFacebook, à queda do valor das ações da empresa e à convocação de Mark Zuckerberg para audiências no Congresso dos Estados Unidos e em parlamentos europeus.

O método utilizado para obtenção dos dados ilustrou uma violação explícita aos princípios de finalidade, necessidade e transparência consagrados na LGPD brasileira. Embora os usuários que acessaram o aplicativo de testes de personalidade tivessem consentido com a coleta de seus dados, não havia clareza sobre o uso posterior das informações, tampouco sobre o acesso estendido aos dados dos amigos da rede social. Essa prática, embora tecnicamente possível à época pela API do Facebook, revela um grave descompasso com os preceitos legais atualmente vigentes no Brasil, especialmente no que diz respeito à exigência de consentimento informado, livre e inequívoco, como estabelece o artigo 7º da Lei nº 13.709/2018 (LGPD).

Segundo Maciel (2020), o escândalo demonstra que o mero aceite de termos genéricos de privacidade não configura um consentimento válido para o tratamento de dados com finalidades tão específicas e sensíveis como o uso político. O caso escancarou a realidade da assimetria informacional entre as plataformas digitais e seus usuários, que, muitas vezes, não compreendem o alcance de suas permissões nem as implicações do uso de seus dados. Ao mesmo tempo, evidenciou a ineficiência de políticas internas de segurança e governança por parte do Facebook, o que permitiu que terceiros violassem os próprios termos da plataforma sem fiscalização efetiva.

A resposta inicial do Facebook foi tardia e hesitante. Em 2018, após as denúncias veiculadas pelo *The Guardian* e pelo *Channel 4 News*, Mark Zuckerberg pediu desculpas publicamente e reconheceu que houve uma “quebra de confiança” entre a empresa e seus usuários. Contudo, a postura inicial da plataforma foi de negar responsabilidade direta, alegando que os dados foram obtidos por meio de consentimento dos usuários e que o desenvolvedor do aplicativo, Aleksandr Kogan, teria descumprido os termos de uso da rede social. Fernandes (2021) destaca que essa

postura revela uma tentativa de esquivar-se da responsabilidade objetiva imposta pelas legislações modernas de proteção de dados.

No Brasil, a repercussão do caso motivou a abertura de um processo administrativo pelo Departamento de Proteção e Defesa do Consumidor (DPDC), sob o número 08012.000723/2018-19, que investigou a prática abusiva e a violação aos direitos dos consumidores brasileiros. Foram exigidos esclarecimentos do Facebook Serviços Online do Brasil Ltda. e da matriz americana, com questionamentos sobre o alcance do vazamento, os mecanismos de consentimento utilizados e a adoção de medidas reparadoras. Conforme relatado pelo portal *GI* (2021), a empresa admitiu que cerca de 443 mil usuários brasileiros podem ter tido seus dados compartilhados indevidamente com a Cambridge Analytica.

As respostas fornecidas pelo Facebook indicaram, em essência, que a responsabilidade pela coleta e uso indevido dos dados seria exclusiva do aplicativo externo. Contudo, essa linha de defesa não foi acolhida pelo DPDC, que, com base no artigo 11 do Marco Civil da Internet (Lei nº 12.965/2014), reconheceu a responsabilidade da subsidiária brasileira por fatos ocorridos no território nacional, dada a existência de representação jurídica local. Barreto e Brasil (2016) apontam que esse tipo de articulação é essencial para a efetividade do ordenamento jurídico em casos que envolvem corporações multinacionais.

Além disso, foi constatado que o consentimento fornecido pelos usuários era genérico e não vinculado a uma finalidade específica, o que caracteriza violação ao artigo 6º da LGPD. A prática adotada pela plataforma feriu também os princípios do Código de Defesa do Consumidor, especialmente no que tange ao dever de transparência e à proteção da boa-fé objetiva nas relações de consumo. O processo concluiu que o Facebook interveio na cadeia de fornecimento do serviço e permitiu o compartilhamento indevido, o que invalidava a tese de que a responsabilidade seria exclusivamente de terceiros.

Com base nesses elementos, o Facebook Inc. e o Facebook Brasil foram condenados ao pagamento de uma multa administrativa no valor de R\$ 6.600.000,00, a ser revertida para o Fundo de Defesa dos Direitos Difusos. A penalidade considerou os critérios de gravidade da infração, vantagem obtida e alcance da lesividade, ainda que a empresa alegasse ser ré primária e ter implementado medidas posteriores de contenção. Como destaca Fernandes (2021), a aplicação de sanções de natureza econômica é uma

das formas mais eficazes de garantir a função pedagógica da norma e desestimular a reincidência de condutas lesivas.

A ausência de uma política de mitigação imediata e a demora em notificar os usuários e as autoridades competentes agravaram a responsabilidade da plataforma. A LGPD brasileira, em seu artigo 48, exige a comunicação tempestiva de incidentes de segurança que possam representar risco ou dano relevante aos titulares dos dados. Segundo Callegari (2019), a notificação tardia demonstra falha no dever de transparência e compromete a confiança dos consumidores, que deixam de ser informados sobre os riscos a que estão submetidos.

No plano internacional, a repercussão do caso motivou a União Europeia a acelerar a implementação do GDPR (Regulamento Geral de Proteção de Dados), que entrou em vigor em maio de 2018. A regulação europeia passou a servir como referência para outras legislações, inclusive a brasileira. Souza, Luíza (2018), ao comparar os dois modelos legais, observa que a necessidade de harmonização normativa é fundamental diante da natureza transnacional dos dados e da atuação global das plataformas digitais.

A exposição de usuários sem seu consentimento específico, associada à utilização de suas informações para manipulação política, comprometeu valores democráticos fundamentais. Como afirma Nascimento (2020), a proteção de dados deve ser vista como um direito fundamental em sociedades digitais, sendo essencial para preservar a liberdade individual e a integridade das instituições. O caso Cambridge Analytica mostrou como o uso indevido de informações pessoais pode influenciar decisões políticas, violando não apenas a privacidade, mas o próprio processo democrático.

A falha do Facebook em garantir a segurança dos dados foi qualificada como prática abusiva, nos termos do artigo 39 do Código de Defesa do Consumidor. Isso se justifica pela ausência de medidas protetivas adequadas e pela omissão em informar os consumidores sobre as implicações do uso de suas informações. Maciel (2020) reforça que o fornecedor de serviços digitais tem o dever legal de adotar políticas de compliance, segurança e governança informacional que garantam o uso lícito e ético dos dados sob sua responsabilidade.

O caso também colocou em evidência a importância da atuação coordenada entre órgãos reguladores, Ministério Público, entidades de defesa do consumidor e a sociedade civil. A denúncia pública e a mobilização dos usuários foram fundamentais

para a responsabilização da plataforma e a abertura de processos investigativos. Segundo Mendes e Branco (2019), a tutela coletiva dos direitos fundamentais é indispensável para assegurar eficácia às normas de proteção de dados em contextos de larga escala.

Por fim, o escândalo Facebook–Cambridge Analytica deixou lições importantes sobre a necessidade de vigilância constante, regulação eficiente e responsabilização exemplar das empresas de tecnologia. Embora o Facebook tenha implementado mudanças internas e reforçado seus controles após o episódio, o caso permanece como símbolo de uma era em que o consentimento era tratado como formalidade e os dados pessoais, como mercadoria.

No Brasil, a condenação administrativa representou um marco relevante, mas não suficiente para resolver todas as vulnerabilidades do sistema. É necessário um fortalecimento contínuo da Autoridade Nacional de Proteção de Dados (ANPD) e da cooperação internacional entre agências reguladoras. Como conclui Fernandes (2021), a era digital exige um novo paradigma jurídico, que reconheça a centralidade dos dados na vida contemporânea e assegure sua proteção como bem jurídico fundamental.

5.2 A atuação da Autoridade Nacional de Proteção de Dados (ANPD) no caso

A criação da Autoridade Nacional de Proteção de Dados (ANPD) pelo artigo 55-A da Lei nº 13.709/2018 (LGPD) representou um avanço significativo no ordenamento jurídico brasileiro, conferindo ao país um órgão regulador específico para fiscalizar, orientar e aplicar sanções no âmbito da proteção de dados pessoais. Embora o escândalo do Facebook–Cambridge Analytica tenha ocorrido antes da efetiva entrada em funcionamento da ANPD, em 2021, sua repercussão foi determinante para acelerar os debates legislativos e reforçar a urgência de uma instância autônoma capaz de lidar com violações dessa magnitude. A atuação da ANPD, mesmo que posterior ao episódio, tornou-se essencial para monitorar a implementação das medidas corretivas prometidas pelas plataformas e prevenir novas violações semelhantes no território nacional.

No Brasil, enquanto a ANPD ainda estava em estruturação, coube ao Departamento de Proteção e Defesa do Consumidor (DPDC), vinculado à Secretaria Nacional do Consumidor (SENACON), a condução do processo administrativo n.º 08012.000723/2018-19. O órgão atuou com base no Código de Defesa do Consumidor

(CDC) e na Lei do Marco Civil da Internet (Lei nº 12.965/2014), solicitando informações do Facebook e apurando possíveis infrações relacionadas à coleta indevida de dados pessoais de usuários brasileiros. A atuação do DPDC teve caráter reativo, limitando-se à aplicação de sanção administrativa, mas abriu espaço para que, futuramente, a ANPD assumisse papel mais estruturante e permanente na regulação do setor.

Com o início de suas atividades em 2021, a ANPD passou a desempenhar função estratégica na análise de políticas de privacidade e medidas de segurança de grandes plataformas digitais, incluindo o Facebook, rebatizado como Meta. No caso em questão, ainda que não tenha conduzido diretamente o processo sancionatório, a ANPD passou a fiscalizar a efetiva adequação da empresa às novas exigências da LGPD, especialmente no que diz respeito à transparência, à finalidade do tratamento de dados e à gestão de consentimento dos titulares. Segundo Maciel (2020), a existência de um órgão técnico e especializado confere maior efetividade à proteção dos dados, pois permite ações mais ágeis e decisões embasadas por critérios jurídicos e tecnológicos consistentes.

Dentre as competências da ANPD listadas no artigo 55-J da LGPD, destacam-se a fiscalização e a aplicação de sanções, a orientação aos agentes de tratamento e a elaboração de relatórios de impacto regulatório. No contexto do caso Facebook–Cambridge Analytica, a autoridade tem a função de verificar se as práticas empresariais atuais da plataforma estão de acordo com os padrões exigidos, especialmente quanto à prevenção de novos vazamentos e à implementação de políticas de segurança mais rigorosas. Além disso, deve assegurar que os titulares de dados tenham acesso a informações claras sobre o tratamento realizado, com possibilidade de exercer seus direitos de forma facilitada.

A atuação da ANPD também se tornou importante para avaliar os mecanismos de cooperação internacional em proteção de dados, uma vez que a empresa envolvida é de origem estrangeira e o tratamento de dados possui alcance global. O artigo 33 da LGPD prevê que o tratamento de dados pessoais poderá ser realizado fora do território nacional apenas quando garantido um nível de proteção adequado. Nesse ponto, a ANPD pode firmar acordos de cooperação com outras autoridades, como a Comissão Europeia, a Federal Trade Commission (FTC) dos Estados Unidos ou entidades britânicas que investigaram diretamente o escândalo. Tais parcerias são fundamentais

para investigar práticas transfronteiriças e assegurar a efetiva responsabilização das empresas em múltiplas jurisdições.

No caso específico do Facebook, a ANPD passou a monitorar a implementação das práticas de segurança prometidas após o escândalo. Entre elas, destacam-se a reformulação do sistema de permissões para aplicativos de terceiros, a limitação de acesso à API da plataforma e a exigência de auditorias regulares sobre o uso dos dados por desenvolvedores. Tais ações foram impulsionadas pela pressão internacional, mas a atuação da ANPD tem contribuído para garantir sua aplicação no Brasil, com base nos artigos 46 a 50 da LGPD, que tratam da segurança e das boas práticas no tratamento de dados.

Outro aspecto relevante da atuação da ANPD no caso diz respeito ao seu papel educativo. A autoridade vem elaborando guias, recomendações e diretrizes voltadas ao setor privado e aos consumidores, com o objetivo de difundir a cultura da proteção de dados e prevenir violações como a do caso Cambridge Analytica. Fernandes (2021) defende que essa atuação preventiva é tão relevante quanto a função sancionadora, pois contribui para a construção de uma cidadania digital consciente e informada. A ANPD também mantém um canal para denúncias e pedidos de titular de dados, promovendo um ambiente mais transparente e participativo.

A atuação da ANPD se mostra ainda mais necessária diante das críticas à alegada “boa-fé” da plataforma no episódio. Durante o processo no Brasil, o Facebook tentou eximir-se de responsabilidade, atribuindo a culpa exclusivamente ao aplicativo “This Is Your Digital Life”. Contudo, a ANPD tem enfatizado que a responsabilidade pelo ecossistema de dados é compartilhada e que os controladores devem fiscalizar os operadores, conforme previsto no artigo 42 da LGPD. Nesse sentido, a autoridade atua não apenas como julgadora de condutas passadas, mas como fiscalizadora de deveres contínuos e preventivos.

A estruturação da ANPD e sua atuação progressiva no caso Cambridge Analytica representam um novo patamar de governança da proteção de dados no Brasil. Embora não tenha sido o órgão originário do processo, a autoridade passou a incorporar suas conclusões e a utilizar o episódio como base para análise de risco e formulação de sua agenda regulatória. Isso inclui, por exemplo, a priorização da fiscalização de grandes plataformas digitais e o estímulo ao desenvolvimento de relatórios de impacto por empresas de tecnologia. O escândalo se tornou, assim, um referencial para a atuação da ANPD no contexto do enforcement da LGPD.

A consolidação da ANPD como órgão independente, técnico e transparente será fundamental para assegurar que episódios como o vazamento de dados do Facebook não se repitam ou, ao menos, sejam devidamente punidos e mitigados. O caso reforça a importância da proteção de dados como direito fundamental e da atuação vigilante do Estado na garantia desse direito, não apenas após o dano, mas principalmente por meio da fiscalização contínua, orientação técnica e promoção de boas práticas de segurança e governança digital.

5.3 Análise jurídica da responsabilidade do Facebook à luz da LGPD

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece um marco normativo robusto sobre a responsabilidade dos agentes de tratamento de dados pessoais no Brasil, conferindo especial atenção ao princípio da responsabilidade e da prestação de contas (art. 6º, inciso X). A partir dessa estrutura legal, é possível realizar uma análise crítica da atuação do Facebook no escândalo de compartilhamento indevido de dados com a Cambridge Analytica, compreendendo as obrigações que foram descumpridas e os fundamentos jurídicos que ensejariam sua responsabilização no cenário pós-LGPD. A conduta da plataforma afronta diversos dispositivos legais e evidencia uma cadeia de falhas que envolvem ausência de consentimento adequado, omissão no dever de informar e ineficiência na governança dos dados.

A LGPD estabelece, em seu artigo 7º, as hipóteses legais para o tratamento de dados pessoais, sendo o consentimento livre, informado e inequívoco um dos pilares da legalidade da operação. No caso do Facebook, os usuários que acessaram o aplicativo “This Is Your Digital Life” consentiram com o fornecimento de seus dados para fins acadêmicos, sem terem sido esclarecidos sobre a real finalidade — a manipulação política e a criação de perfis comportamentais com fins eleitorais. Segundo Maciel (2020), esse tipo de consentimento genérico e enganoso fere o princípio da transparência e compromete a legalidade do tratamento, tornando-o ilícito à luz da LGPD.

Além disso, a plataforma permitiu, via sua API, o acesso a dados não apenas do usuário que consentiu diretamente, mas também de seus contatos e conexões na rede social, sem o devido consentimento desses terceiros. Isso viola expressamente o artigo 8º, §4º da LGPD, que condiciona a validade do consentimento à sua vinculação direta

com a finalidade e à manifestação individualizada do titular. Conforme observa Fernandes (2021), qualquer extensão do uso de dados sem o conhecimento do titular compromete os fundamentos da autodeterminação informativa, uma das bases filosóficas e jurídicas da proteção de dados.

Do ponto de vista da segurança da informação, o Facebook descumpriu o dever previsto no artigo 46 da LGPD, que impõe aos controladores e operadores a obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. O fato de a plataforma não ter detectado nem impedido o uso indevido dos dados por terceiros evidencia uma falha grave em sua política de compliance digital. Boiteux (2010) já apontava a importância de estruturas de governança eficazes como condição essencial para a proteção de dados no contexto de grandes corporações multinacionais.

No tocante à responsabilização civil, o artigo 42 da LGPD é claro ao dispor que o agente de tratamento que causar dano patrimonial, moral, individual ou coletivo em decorrência do tratamento de dados em desconformidade com a lei, responde pela reparação dos danos. Trata-se de responsabilidade que, conforme o parágrafo 1º do referido artigo, pode ser solidária quando houver mais de um agente envolvido. Nesse contexto, tanto o Facebook quanto o desenvolvedor do aplicativo podem ser responsabilizados, sem prejuízo do direito de regresso. Segundo Barreto (2020), a responsabilização solidária é fundamental para evitar lacunas de responsabilização e proteger os direitos dos titulares com maior efetividade.

Outro ponto jurídico relevante é a ausência de comunicação imediata aos titulares e às autoridades competentes acerca do incidente de segurança, o que caracteriza violação ao artigo 48 da LGPD. A omissão em comunicar o vazamento em tempo hábil agrava a posição jurídica do controlador, evidenciando má-fé ou, no mínimo, negligência. Como destaca Callegari (2019), a transparência na gestão de crises é não apenas um dever legal, mas um requisito para reconstrução da confiança entre consumidores e provedores de serviço.

No Brasil, o processo administrativo n.º 08012.000723/2018-19, conduzido pelo DPDC, concluiu pela aplicação de multa ao Facebook por práticas abusivas e violação à boa-fé contratual, à luz do Código de Defesa do Consumidor (CDC). O órgão entendeu que a empresa não apenas falhou em informar adequadamente os usuários sobre o uso de seus dados, mas também permitiu o acesso por terceiros sem mecanismos de controle suficientes. Barreto e Brasil (2016) defendem que, em situações como essa, a aplicação

concomitante da LGPD e do CDC é legítima, dada a relação de consumo existente entre usuário e plataforma digital.

Mesmo que o Facebook tenha alegado que a coleta foi realizada por um terceiro, a LGPD impõe ao controlador o dever de diligência sobre os operadores e desenvolvedores externos. A responsabilidade pelo ecossistema de dados é intransferível e inalienável, conforme estabelece o artigo 50, que trata da adoção de boas práticas e governança. Nesse sentido, Bomfati e Kolbe Junior (2020) destacam que plataformas digitais devem manter uma política ativa de auditoria e fiscalização sobre quem acessa e utiliza seus dados, sob pena de responderem civil e administrativamente por condutas de terceiros.

A tentativa de isenção de responsabilidade da filial brasileira da plataforma, baseada na alegação de que os fatos foram praticados pela matriz estrangeira, também encontra resistência jurídica. O artigo 11 do Marco Civil da Internet impõe a aplicação da legislação brasileira sempre que a coleta de dados se der em território nacional ou atingir brasileiros. Essa regra de territorialidade foi decisiva para que a atuação do Facebook Brasil também fosse incluída no processo, reforçando a responsabilização do grupo econômico. Conforme argumenta Nascimento (2020), a proteção de dados pessoais deve ser compreendida como direito fundamental que não se esgota na jurisdição formal, mas acompanha o titular onde ele estiver.

A ausência de finalidade legítima e de adequação no uso dos dados, conforme previsto no artigo 6º, incisos I e II da LGPD, reforça a ilicitude do tratamento promovido pela Cambridge Analytica com a anuência ou conivência da plataforma. Os dados não foram utilizados para os fins que foram declarados aos usuários, mas sim para manipulação eleitoral. Essa ruptura entre a promessa e a prática caracteriza infração grave à norma, conforme sustentam Fernandes (2021) e Pinheiro (2021), que enfatizam o papel central da confiança nas relações de tratamento de dados pessoais.

A análise jurídica da responsabilidade do Facebook à luz da LGPD revela uma série de infrações que justificariam sua responsabilização civil, administrativa e possivelmente penal, a depender das circunstâncias de cada país. No Brasil, embora o escândalo tenha ocorrido antes da plena vigência da LGPD, seus efeitos permanecem atuais, sendo utilizados como paradigma para decisões regulatórias e como exemplo da necessidade de se fortalecer a atuação da Autoridade Nacional de Proteção de Dados (ANPD), conforme destaca Mendes e Branco (2019).

Por fim, é necessário reconhecer que o caso Facebook–Cambridge Analytica não foi um episódio isolado, mas a manifestação de um modelo de negócio baseado na exploração massiva de dados pessoais, muitas vezes em desacordo com os princípios constitucionais da dignidade da pessoa humana e da inviolabilidade da intimidade. A responsabilidade jurídica do Facebook, portanto, não pode ser vista apenas sob a ótica compensatória, mas também como instrumento para prevenir novas violações e reequilibrar as relações entre consumidores e corporações na sociedade da informação.

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo central analisar os fundamentos da responsabilidade civil das plataformas digitais diante do compartilhamento indevido de dados pessoais, com base na Lei Geral de Proteção de Dados (LGPD), tomando como estudo de caso o escândalo envolvendo o Facebook e a Cambridge Analytica. Ao longo do trabalho, constatou-se que a LGPD representa um avanço normativo importante no ordenamento jurídico brasileiro, ao consolidar princípios como o da transparência, finalidade, responsabilização e segurança, cuja violação configura hipótese clara de responsabilização do agente de tratamento. O caso estudado revelou a urgência da efetiva implementação da legislação, sobretudo diante do poder concentrado nas mãos de grandes corporações tecnológicas, cujas atividades impactam direta e coletivamente os direitos fundamentais dos titulares.

A análise crítica dos fatos relacionados ao escândalo Cambridge Analytica demonstrou que o Facebook, ao permitir o acesso a dados de milhões de usuários sem consentimento informado, incorreu em diversas infrações à LGPD. Mesmo que o incidente tenha ocorrido em momento anterior à vigência formal da lei, sua repercussão serve como paradigma para as hipóteses de responsabilização contemporâneas. Ficou evidenciado que houve falhas estruturais tanto na coleta quanto na governança dos dados, além da ausência de mecanismos eficazes de auditoria sobre terceiros com acesso à plataforma. Tais lacunas comprometem a integridade do sistema de proteção de dados e expõem a vulnerabilidade dos usuários diante de práticas abusivas e opacas.

A responsabilização civil da plataforma, à luz da LGPD, encontra respaldo legal nos dispositivos que tratam da reparação de danos, especialmente o artigo 42, que prevê tanto a responsabilidade subjetiva quanto a objetiva, conforme o tipo de violação. A

obrigação de indenizar danos patrimoniais e morais, individuais ou coletivos, revela a preocupação da legislação em garantir efetividade à tutela de direitos. No caso em questão, a responsabilização não se limita ao aspecto compensatório, mas deve também cumprir função pedagógica e preventiva, desestimulando condutas semelhantes por parte de outras plataformas e fomentando uma cultura de respeito aos dados pessoais.

O estudo também demonstrou a importância do papel da Autoridade Nacional de Proteção de Dados (ANPD) no fortalecimento do sistema de governança digital no Brasil. Embora não tenha sido a responsável direta pela condução do processo administrativo referente ao escândalo, a ANPD tem contribuído de forma estratégica para a consolidação da cultura de proteção de dados, mediante orientações, fiscalizações e estímulo à autorregulação. A sua atuação técnica e independente é essencial para garantir o cumprimento efetivo da LGPD e assegurar que as plataformas digitais adotem medidas robustas de compliance, transparência e segurança informacional.

Outro ponto relevante das conclusões é o reconhecimento da importância do consentimento como base legal para o tratamento de dados pessoais. No entanto, conforme demonstrado no estudo, o consentimento deve ser efetivamente informado, específico e livre, não podendo ser presumido ou derivado de termos genéricos de uso. O caso Facebook exemplifica como consentimentos obtidos de forma inadequada podem resultar em violações massivas, tornando evidente a necessidade de revisão e fiscalização rigorosa das práticas adotadas pelas plataformas, sobretudo no que diz respeito a políticas de privacidade, permissões de aplicativos e coleta de dados indireta.

Ademais, foi possível identificar que a responsabilização jurídica das plataformas digitais precisa ser compreendida dentro de uma lógica de ecossistema de dados, onde os controladores devem exercer diligência sobre todos os agentes envolvidos no tratamento. A tentativa de transferência de responsabilidade para desenvolvedores terceiros não se sustenta juridicamente quando se considera que a plataforma criou as condições técnicas para o compartilhamento indevido e não implementou mecanismos eficazes de prevenção. A jurisprudência e a doutrina contemporânea têm apontado nesse mesmo sentido, reforçando a ideia de corresponsabilidade entre os entes que participam da cadeia de tratamento de dados.

Neste interim, a pesquisa conclui que a responsabilidade civil das plataformas digitais é um instrumento indispensável para a consolidação de um ambiente digital mais ético, seguro e juridicamente equilibrado. O caso analisado reforça a necessidade de maior vigilância por parte do Estado, da sociedade civil e dos próprios usuários, além

da adoção de práticas regulatórias mais severas e transparentes. A responsabilização, nesse contexto, não visa apenas punir, mas promover a confiança dos cidadãos na economia digital, fortalecendo os direitos informacionais e a cidadania na era da informação.

Assim, a partir da análise do caso Facebook–Cambridge Analytica à luz da LGPD, conclui-se que a responsabilização civil das plataformas digitais não é apenas juridicamente viável, como também necessária para o cumprimento dos objetivos da proteção de dados pessoais no Brasil. A pesquisa reafirma o valor dos dados como patrimônio sensível do indivíduo e destaca a urgência de garantir que sua proteção não dependa apenas de termos contratuais, mas de um compromisso institucionalizado com os direitos fundamentais da pessoa humana.

REFERENCIAS

ALVES, Matheus de Araújo. *Crimes digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Criminal e do Instituto da Prova*. 1ª ed. São Paulo: Dialética, 2020.

ANDRION, Roseli. O que é stalking? Como se proteger? Canaltech, 2021. Disponível em: <https://canaltech.com.br/seguranca/o-que-e-stalking-como-se-proteger-205060/>. Acesso em: 11 abr. 2025. [Jus Navigandi+7Jusbrasil+7Jusbrasil+7](#)

BAPTISTA, Ricardo Córdoba. Crime de participação em suicídio ou automutilação: inovações da Lei 13.968/2020. Jus.com.br, 2020. Disponível em: <https://jus.com.br/artigos/83419/crime-de-participacao-em-suicidio-ou-automutilacao-inovacoes-da-lei-13-968-2020>. Acesso em: 01 abr. 2025.

BAPTISTA, Ricardo Córdoba. O que é ciberextorsão? My.cybersecurity, 2016. Disponível em: <https://www.mycybersecurity.com.br/o-que-e-ciber-extorsao/>. Acesso em: 02 abr. 2025. [Jus Navigandi+7Jusbrasil+7Jusbrasil+7](#)

BARBOSA, Igor Gabriell Siqueira. A proteção de dados pessoais como um direito fundamental à luz da Constituição Federal de 1988. 43f. 2021. Monografia (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1474/1/TCC%20II%20-%20TURMA%20B12%20-%20IGOR%20GABRIELL%20-%20ARTIGO-2021-1%29.pdf>. Acesso em: 02 abr. 2025.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética à luz do marco civil da internet*. 1ª ed. Rio de Janeiro: Brasport, 2016.

BARRETO, Alesandro Gonçalves. *Ciber Crimes e seus reflexos no direito brasileiro*. Salvador: Editora JusPodivm, 2020.

BARROS, Thiago. Facebook diz que não há violação de segurança ou privacidade de dados dos usuários. 2011. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2011/09/facebook-confirma-que-botao-curtir-repassa-dados-dos-usuarios-e-promete-correcao-dos-cookies.html>. Acesso em: 15 mar. 2025.

BITENCOURT, Cezar Roberto. Furto mediante uso de dispositivo eletrônico ou informático. Consultor Jurídico, 2021. Disponível em: <https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico/>. Acesso em: 22 fev. 2025.

BITTENCOURT, Rodolfo P. P. O anonimato, a liberdade, a publicidade e o direito eletrônico. Jusbrasil, 2016. Disponível em: <https://www.jusbrasil.com.br/artigos/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico/371604693>. Acesso em: 01 abr. 2025. [Jus Navigandi+7Jusbrasil+7Jusbrasil+7](#)

BOITEUX, L. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. *Doutrinas Essenciais de Direito Penal*, v. 8, 2010.

BOMFATI, Cláudio Adriano; KOLBE JUNIOR, Armando. *Crimes Cibernéticos*. Curitiba: Intersaberes, 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 jan. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 mar. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 07 abr. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 07 abr. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 9 abr. 2025. Jus Navigandi+7Jusbrasil+7Jusbrasil+7

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 11 abr. 2025.

BRASIL. *Lei nº 13.869, de 5 de setembro de 2019*. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), entre outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113869.htm. Acesso em: 11 abr. 2025.

BRASIL. *Lei nº 14.155, de 27 de maio de 2021*. Altera o Código Penal para agravar penas de crimes cometidos com uso de dispositivo eletrônico ou informática. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 12 abr. 2025.

BRASIL. Lei nº 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências.

Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em: 4 fev. 2025.

BRASIL. *Marco Civil da Internet. Lei nº 12.965, de 23 de abril de 2014*. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 abr. 2025.

CALLEGARI, André Luís. *Crimes cibernéticos e a nova realidade digital*. São Paulo: Revista dos Tribunais, 2019.

CONJUR. Protógenes Queiroz é demitido da PF por uso indevido do cargo. Revista Consultor Jurídico, 14 out. 2015. Disponível em: <https://www.conjur.com.br/2015-out-14/protogenes-queiroz-demitido-pf-uso-indevido-cargo>. Acesso em: 05 abr. 2025.

CONVERGÊNCIA DIGITAL. Justiça não poupa Google e mantém processo por venda de dados pessoais. 2015. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=39306&sid=17#.VSKAPfzF_EU. Acesso em: 09 abr. 2025.

DA COSTA, Fernando José. Locus delicti nos crimes informáticos. 2011. 355f. Tese (Doutorado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php>. Acesso em: 20 abr. 2025.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades». G1.

Facebook scandal 'hit 87 million users» (em inglês). BBC News.

FERNANDES, Douglas. *Crimes cibernéticos: aspectos penais e processuais penais da criminalidade informática*. 2. ed. São Paulo: Saraiva, 2021.

GONÇALVES, Andressa Ferraz. Análise dos Direitos Fundamentais no Âmbito Digital e a Punição Estatal. Revista Aporia Jurídica, v. 1, p. 8-25, 2018. Disponível em: <http://cescage.com.br/revistas/index.php/aporiajuridica/article/download/136/135>. Acesso em: 21 abr. 2025.

GONZAGA, Yuri. Justiça suspende decisão de remover Secret no Brasil após pedido do Google. *Folha de São Paulo*, 2014. Disponível em: <https://m.folha.uol.com.br/tec/2014/09/1515215-justica-suspende-decisao-de-remover-secret-no-brasil-apos-pedido-do-google.shtml>. Acesso em: 24 abr. 2025.

How Trump Consultants Exploited the Facebook Data of Millions» (em inglês). The New York Times.

LUZ, Saulo. ESTADÃO: Cuidado, seus dados pessoais estão à venda. São Paulo, fev. 2012. Disponível

em: <https://www.estadao.com.br/blogs/jt-seu-bolso/2012/02/12/cuidado-seus-dados-pessoais-estao-a-venda/>. Acesso em: 15 abr. 2025.

MACIEL, Rafael Fernandes. *Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)*. 2. ed. Goiânia: RM Digital Education, 2020.
DOI: <https://doi.org/10.32586/rcda.v18i1.588>.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 14. ed. São Paulo: Saraiva, 2019.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Panorama Setorial da Internet*, Brasília, n. 2, jun. 2019.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP). *Cartilha de segurança para internet*. CERT.br, 2023. Disponível em: <https://cartilha.cert.br/>. Acesso em: 11 abr. 2025.

MIRAGAIA, Bruno Ricardo; BELMUDES, Eduardo. Com o dever de proteger direitos humanos, Estado é o maior violador. *Consultor Jurídico*, São Paulo, 2008. Disponível em: https://www.conjur.com.br/2008-dez-26/estado_maior_violador_direitos_humanos. Acesso em: 14 abr. 2025.

NASCIMENTO, Rogério Greco do. *Crimes cibernéticos e a Constituição Federal de 1988: uma análise sob a ótica dos direitos fundamentais*. Belo Horizonte: Del Rey, 2020.

PINHEIRO, Patrícia P. *Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Editora Saraiva, 2021.

PORTAL G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. 2013. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 22 mar. 2025.

SILVA, De Plácido e. *Vocabulário Jurídico*. 28. ed. Rio de Janeiro: Forense, 2021.

SIMON, Joel. Como a espionagem dos Estados Unidos fortalece o controle da China. *Committee to Protect Journalists*, 2014. Disponível em: <https://cpj.org/pt/2014/02/ataque-a-imprensa-em-2013-como-a-espionagem/>. Acesso em: 22 mar. 2025.

SOUZA, Luíza Ribeiro de Menezes. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016. *Caderno Virtual*, v. 1, n. 41, 2018.

SOUZA, Marília dos Santos. *A internet e os crimes virtuais: desafios para o Direito Penal*. Rio de Janeiro: Lumen Juris, 2020.

Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users» (em inglês). The Guardian.