UNIVERSIDADE FEDERAL DE GOIÁS
CAMPUS CIDADE DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO

BRUNA FRAGA SIQUEIRA CAVALCANTI

RESPONSABILIDADE CIVIL NA ERA DAS INTELIGÊNCIAS ARTIFICIAIS:
análise da coleta indevida de dados pessoais no Brasil e o caso TikTok

GOIÁS
2024

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome completo da autora: Bruna Fraga Siqueira Cavalcanti

Título do trabalho: Responsabilidade civil na era das inteligências artificiais: análise da coleta indevida de dados pessoais no Brasil e o caso TikTok

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Bruna Pinotti Garcia**, **Professora do Magistério Superior**, em 29/01/2025, às 15:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Bruna Fraga Siqueira Cavalcanti**, **Discente**, em 29/01/2025, às 15:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5045564** e o código CRC **92C200F5**.

Referência: Processo nº 23070.064142/2024-52 SEI nº 5045564

BRUNA FRAGA SIQUEIRA CAVALCANTI

RESPONSABILIDADE CIVIL NA ERA DAS INTELIGÊNCIAS ARTIFICIAIS: análise da coleta indevida de dados pessoais no Brasil e o caso TikTok

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Goiás, Campus Goiás, como requisito parcial para obtenção do grau de bacharel em Direito, sob orientação da Profa. Dra. Bruna Pinotti Garcia.

GOIÁS
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Cavalcanti, Bruna Fraga Siqueira
Responsabilidade civil na era das inteligências artificiais: análise da coleta indevida de dados pessoais no Brasil e o caso TikTok [manuscrito] / Bruna Fraga Siqueira Cavalcanti. - 2024.
79 f.

Orientador: Profa. Dra. Bruna Pinotti Garcia.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2024.
Anexos.

1. Responsabilidade civil. 2. Inteligência artificial. 3. Proteção de dados. 4. Coleta indevida. 5. TikTok. I. Garcia, Bruna Pinotti, orient. II. Título.

CDU 34

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos treze dias do mês de dezembro do ano de dois mil e vinte e quatro iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado “Responsabilidade civil na era das inteligências artificiais: análise da coleta indevida de dados pessoais no Brasil e o caso TikTok”, de autoria de Bruna Fraga Siqueira Cavalcanti, do curso de Direito, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas do Câmpus Goiás da UFG. Os trabalhos foram instalados pela Dra. Bruna Pinotti Garcia – orientadora (UAECSA/UFG) com a participação dos demais membros da Banca Examinadora: Dra. Renata Botelho Dutra e Dra. Sofia Alves Valle Ornelas. Posteriormente a Banca Examinadora APROVOU o TCC.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Renata Botelho Dutra**, **Professora do Magistério Superior**, em 15/01/2025, às 21:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Bruna Pinotti Garcia**, **Professora do Magistério Superior**, em 29/01/2025, às 15:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Sofia Alves Valle Ornelas**, **Professora do Magistério Superior**, em 29/01/2025, às 18:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5045563** e o código CRC **4529D7C2**.

AGRADECIMENTOS

À minha família, que sempre me deu incentivo, apoio e equilíbrio.

Aos meus amigos, que sempre estiveram ao meu lado.

À minha orientadora, fonte de inspiração.

E a todos que, direta ou indiretamente, me auxiliaram na elaboração deste trabalho.

Sem vocês, nada seria possível.

[...] E todo anelo é cego, salvo quando há conhecimento.
E todo conhecimento é vão, salvo quando há trabalho;
E todo trabalho é vazio, salvo quando há amor [...]
Khalil Gibran

RESUMO

A presente monografia analisa a aplicação da responsabilidade civil no contexto das inteligências artificiais (IA´s), com ênfase na coleta indevida de dados pessoais e nos desafios jurídicos decorrentes das práticas tecnológicas disruptivas, evidenciando a opacidade algorítmica e a ausência de normas específicas para regulamentar seu desenvolvimento e funcionamento. Como referência, abordar-se-á a condenação da plataforma TikTok pela coleta indevida de dados pessoais sensíveis, realizada sem o consentimento inequívoco dos titulares. Dividido em três capítulos, o trabalho revisita os fundamentos da responsabilidade civil, explorando seus elementos essenciais – conduta humana, dano, nexo causal e culpa –, e examinando os entraves para a aplicação às tecnologias emergentes. Em seguida, investiga os marcos normativos brasileiros voltados à proteção de dados, com destaque para o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. O último capítulo aprofunda-se no caso TikTok, apurando as irregularidades identificadas, a responsabilização da plataforma e os reflexos desse episódio para a regulação das IA´s e a proteção de dados pessoais. Conclui-se que, embora a responsabilidade civil forneça uma base relevante para mitigar os danos advindos dos sistemas inteligentes, a ausência de regulamentação específica compromete a segurança jurídica e a tutela de direitos fundamentais. O estudo destaca a necessidade de aprimoramento legislativo para abarcar as particularidades das IA´s, conciliando inovação tecnológica e proteção da dignidade humana, no ambiente digital.

Palavras-chave: Responsabilidade civil. Inteligência artificial. Proteção de dados. Coleta indevida. TikTok.

ABSTRACT

The present monograph examines the application of civil liability in the context of artificial intelligence (AI), with an emphasis on the improper collection of personal data and the legal challenges arising from disruptive technological practices, highlighting algorithmic opacity and the absence of specific regulations to govern its development and operation. As a reference, the study addresses the conviction of the TikTok platform for the improper collection of sensitive personal data conducted without the unequivocal consent of data subjects. Divided into three chapters, the work revisits the foundations of civil liability, exploring its essential elements – human conduct, damage, causal link, and fault – and examining the obstacles to its application to emerging technologies. Subsequently, it investigates Brazilian legal frameworks for data protection, with emphasis on the Consumer Defense Code, the Internet Civil Framework, and the General Data Protection Law. The final chapter delves into the TikTok case, investigating the identified irregularities, the platform's accountability, and the implications of this episode for AI regulation and personal data protection. It concludes that, although civil liability provides a relevant basis for mitigating the damages arising from intelligent systems, the absence of specific regulations undermines legal security and the protection of fundamental rights. The study highlights the need for legislative improvement to address the peculiarities of AI, reconciling technological innovation with the protection of human dignity in the digital environment.

KEYWORDS: Civil liability. Artificial intelligence. Data protection. Improper data collection. TikTok.

LISTA DE ABREVIATURAS E SIGLAS

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

ART – *ACCOUNTABILITY, RESPONSIBILITY AND TRANSPARENCY*

CC – CÓDIGO CIVIL

CDC – CÓDIGO DE DEFESA DO CONSUMIDOR

CRFB – CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL

FTC - *FEDERAL TRADE COMMISSION*

GDPR - *GENERAL DATA PROTECTION REGULATION*

IA – INTELIGÊNCIA ARTIFICIAL

LGPD – LEI GERAL DA PROTEÇÃO DE DADOS PESSOAIS

MCI – MARCO CIVIL DA INTERNET

PL – PROJETO DE LEI

RGPD - REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

STJ – SUPERIOR TRIBUNAL DE JUSTIÇA

SUMÁRIO

INTRODUÇÃO

A inteligência artificial (IA) desponta como uma das mais marcantes inovações tecnológicas do Século XXI, desencadeando transformações profundas em setores essenciais, como saúde, transporte, educação e comunicação. Em âmbito global, nações como os Estados Unidos e a China destacam-se pelo investimento maciço em pesquisa e desenvolvimento, reconhecendo o potencial econômico e estratégico dessa tecnologia disruptiva (LEE, 2019). Contudo, o avanço vertiginoso das tecnologias inteligentes também traz à tona desafios éticos e jurídicos de elevada complexidade, especialmente no que concerne à proteção de dados pessoais. A utilização de sistemas que manipulam vastos volumes de informações, associada à opacidade dos algoritmos, evidencia deficiências nos mecanismos de salvaguarda jurídica e aumenta a vulnerabilidade dos titulares de dados diante de práticas possivelmente abusivas.

Dentro desse panorama, o caso TikTok emerge como um exemplo emblemático que ilustra os desafios enfrentados pelo ordenamento jurídico, na proteção de dados pessoais e na responsabilização por práticas ilícitas. A plataforma foi condenada pela coleta reiterada de dados sensíveis, como a biometria facial, sem o consentimento livre, inequívoco e informado de seus usuários. A conduta transgrediu não apenas dispositivos constitucionais e infraconstitucionais, mas também evidenciou a ineficiência dos mecanismos de transparência supostamente adotados pela empresa. Outrossim, o julgamento delineou a urgência de regulamentações mais rígidas, e de um fortalecimento institucional que harmonize a inovação tecnológica com a proteção dos direitos fundamentais. As repercussões do caso transcendem a esfera individual, revelando impactos coletivos que reforçam a necessidade de ajustes legislativos e de políticas regulatórias robustas.

Neste cenário, a presente pesquisa propõe-se a examinar a adequação dos institutos jurídicos tradicionais ao tratamento das complexidades impostas pela inteligência artificial, com ênfase na responsabilização civil, em casos de coleta inadequada de dados pessoais. No Brasil, a ausência de uma regulamentação específica para IA intensifica os desafios, tornando o caso TikTok um paradigma que explicita tanto os limites das normas atualmente vigentes, quanto a necessidade de reformas que contemplem as particularidades das tecnologias emergentes. Avaliar-se-á em que medida os institutos clássicos da responsabilidade civil - conduta, ato ilícito, nexo causal e dano -, podem ser adaptados às novas demandas tecnológicas.

Sob essa conjuntura, a análise recairá sobre os principais instrumentos normativos aplicáveis à proteção de dados no Brasil, notadamente o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados (LGPD). Busca-

se compreender se os referidos marcos regulatórios, em sua configuração atual, são capazes de oferecer uma tutela jurídica eficaz, ou se é imprescindível a criação de uma legislação específica que aborde as peculiaridades das tecnologias inteligentes e seus impactos.

A metodologia empregada é de abordagem qualitativa, alicerçada no exame bibliográfico e documental. A fundamentação teórica recorre a autores renomados, como Gustavo Tepedino, Danilo Doneda e Laura Schertel Mendes, enquanto o caso TikTok é utilizado como referência empírica para ilustrar as dificuldades práticas enfrentadas pelo ordenamento jurídico brasileiro. A escolha permite destacar tanto os limites do arcabouço normativo vigente, quanto as oportunidades de adaptação legislativa que promovam um equilíbrio entre inovação tecnológica e garantia de direitos fundamentais.

A estrutura do estudo foi traçada em três capítulos principais. No primeiro, são revisitados os fundamentos da responsabilidade civil no direito brasileiro, abordando seus elementos essenciais, suas modalidades e suas funções, tanto no contexto tradicional quanto em cenários inovadores. O segundo capítulo concentra-se no exame do arcabouço normativo aplicável ao tratamento e à proteção de dados, com especial atenção ao CDC, ao Marco Civil da Internet e à LGPD. Finalmente, o terceiro capítulo é dedicado à análise do caso TikTok, investigando as irregularidades constatadas, a responsabilização da empresa e o precedente estabelecido, para o campo jurídico, relacionado à inteligência artificial e proteção de dados.

Desse modo, a relevância da presente pesquisa está em situar o tema no centro das discussões acerca da convergência entre progresso tecnológico e proteção jurídica. Ao longo da arguição, será demonstrada a importância da proteção de dados pessoais como um dos pilares da dignidade humana, na era digital, além de destacar a necessidade de ajustes normativos para garantir um ambiente regulatório eficaz e seguro, capaz de acompanhar os avanços tecnológicos sem negligenciar direitos fundamentais.

CAPÍTULO 1 – FUNDAMENTOS DA RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO

A priori, destaca-se que o instituto da responsabilidade civil, tal como é conhecido nos dias hodiernos, passou por inúmeras transformações, que acompanharam as evoluções histórico-culturais da sociedade como um todo. Assim, ressalta-se que tal construção jurídica é fruto das adaptações sofridas com o passar do tempo, que se adequaram ao modelo social adotado. Indubitavelmente, existe a constante busca pela restauração do equilíbrio desfeito por ocasião de danos, em suas diferentes extensões e implicações.

Historicamente, as primeiras formas organizadas de sociedade baseavam-se na ideia de vingança, como reação pessoal ao prejuízo sofrido. A concepção de delito, trazida pelo Direito Romano, ressaltava, justamente, tal possibilidade de comportamento, ao inserir a Pena de Talião, que remonta à Lei das XII Tábuas (olho por olho, dente por dente). Ainda neste caminhar, identificou-se, como aprimoramento da abordagem instituída, a possibilidade de composição obrigatória e tarifada entre as partes envolvidas, com a fixação de multa pecuniária, a ser adimplida pelo ofensor. Alvino Lima *apud* Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 56) destaca:

> [...] este período sucede o da composição tarifada, imposto pela Lei das XII Tábuas, que fixava, em casos concretos, o valor da pena a ser paga pelo ofensor. É a reação contra a vingança privada, que é assim abolida e substituída pela composição obrigatória. Embora subsista o sistema do delito privado, nota-se, entretanto, a influência da inteligência social, compreendendo-se que a regulamentação dos conflitos não é somente uma questão entre particulares. A Lei das XII Tábuas, que determinou o *quantum* para a composição obrigatória, regulava casos concretos, sem um princípio geral fixador da responsabilidade civil. A *actio de reputis sarciendi*, que alguns afirmam que consagrava um princípio de generalização da responsabilidade civil, é considerada, hoje, como não contendo tal preceito (Lei das XII Tábuas — Tábua VIII, Lei 5.ª).

Posteriormente, vislumbrou-se a edição da *Lex Aquilia,* segundo a qual buscava-se o estabelecimento de penas pecuniárias proporcionais aos danos causados, afastando as reparações em valores fixos. Passa-se a identificar, paulatinamente, o elemento "culpa", de modo que, a partir da análise do prejuízo concreto, quantifica-se a indenização efetiva da vítima do evento danoso, com ressarcimento compatível ao caso. Ainda segundo Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 56-57):

> Constituída de três partes, sem haver revogado totalmente a legislação anterior, sua grande virtude é propugnar pela substituição das multas fixas por uma pena

> proporcional ao dano causado. Se seu primeiro capítulo regulava o caso da morte dos escravos ou dos quadrúpedes que pastam em rebanho; e o segundo, o dano causado por um credor acessório ao principal, que abate a dívida com prejuízo do primeiro; sua terceira parte se tornou a mais importante para a compreensão da evolução da responsabilidade civil. Com efeito, regulava ela o *damnum injuria datum*, consistente na destruição ou deterioração da coisa alheia por fato ativo que tivesse atingido coisa corpórea ou incorpórea, sem justificativa legal. Embora sua finalidade original fosse limitada ao proprietário de coisa lesada, a influência da jurisprudência e as extensões concedidas pelo pretor fizeram com que se construísse uma efetiva doutrina romana da responsabilidade extracontratual.

A referida evolução no regime de responsabilidade civil foi incorporada pelo Código de Napoleão que, regido pelos Princípios da Liberdade, Igualdade e Fraternidade, inspirou a legislação civil moderna do Brasil. Este, em seu Artigo 1.382, consolidou o critério geral e abstrato de responsabilização, fundado na ideia de culpa aquiliana. Dessa forma, há a expressa previsão de que os danos causados, efetivamente e culposamente, a outrem, devem ser reparados. Existe a transmutação do caráter punitivo para o caráter compensativo, como preceitua Wendell Lopes Barbosa de Souza (2015, p. 18-19), com a distinção entre as esferas penal e civil.

Reitera-se, nesse ponto, que, apesar dos avanços significativos vislumbrados com a Revolução Francesa, e o singular *Code Napoléon*, foram identificadas várias lacunas na aplicação da responsabilidade civil, especialmente com o advento da Revolução Industrial, em meados do Século XVIII, que emergiu situações, tais como acidentes de trabalho, que não se enquadravam no conceito subjetivo anteriormente difundido. Inegavelmente, havia-se a necessidade de busca por soluções alternativas à dificuldade no estabelecimento do culpado pelos infortúnios trazidos (SOUZA, 2015, p. 21).

Destacam-se novas adaptações jurídicas que, progressivamente, ampararam a presente teoria da responsabilidade civil, no âmbito do Direito Civil Brasileiro. Apesar da perpetuação de divergências doutrinárias, no que tange aos elementos estruturais, entende-se, de forma unânime, que a obrigação de indenizar decorre do descumprimento de dever jurídico anterior, seja ele contratual ou extracontratual, objetivo ou subjetivo. Segundo Sérgio Cavalieri Filho (2012, p. 2):

> É aqui que entra a noção de responsabilidade civil. Em seu sentido etimológico, responsabilidade exprime a ideia de obrigação, encargo, contraprestação. Em sentido jurídico, o vocábulo não foge dessa ideia. A essência da responsabilidade está ligada à noção de desvio de conduta, ou seja, foi ela engendrada para alcançar as condutas praticadas de forma contrária ao direito e danosas a outrem. Designa o dever que alguém tem de reparar o prejuízo decorrente da violação de um outro dever jurídico. Em apertada síntese, responsabilidade civil é um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário.

Ademais, acompanhando a linha histórica, é inegável que a chamada Terceira Revolução Industrial, ocorrida em meados do Século XX, e também conhecida como Revolução Tecnológica, impactou profundamente a forma como o direito regula as novas esferas sociais. O avanço das tecnologias digitais continua a influenciar a sociedade até os dias de hoje, suscitando debates jurídicos atuais, especialmente no que se refere aos danos causados por essas inovações.

Nesse contexto, destacam-se as inteligências artificiais, amplamente adotadas por empresas e plataformas digitais para processar grandes volumes de informações. Contudo, a autonomia dessas tecnologias levanta questões sobre a coleta indevida de dados pessoais, especialmente quando realizada sem consentimento expresso, ou transparência. Ferramentas de IA são capazes de monitorar, armazenar e analisar dados dos usuários de forma automatizada, o que pode resultar em violações à privacidade. Danilo Doneda e Laura Schertel Mendes (DONEDA; MENDES, 2018, s.p.) consideram que o tratamento de dados carrega um risco inerente, tendo em vista que a violação desses direitos pode resultar em prejuízos expressivos, devido à sua natureza de direitos personalíssimos e fundamentais.

Concomitantemente, paira-se a dúvida sobre a aplicação da responsabilidade civil, afinal, a coleta de dados pode ocorrer sem a intervenção humana direta, tornando difícil identificar o responsável pelo dano. Em suma, o capítulo inicial do presente trabalho abordará, especialmente, os conceitos tradicionais do instituto da responsabilidade civil, fomentando a futura discussão sobre como estes poderão ser aplicados no contexto atual, onde a coleta de dados pessoais, através de inteligências artificiais, ganha potencial relevância.

1.1 Elementos Estruturais do Instituto da Responsabilidade Civil

A responsabilidade civil, no ordenamento jurídico brasileiro, é estudada com base em elementos estruturais que, se identificados no caso concreto, ensejam o dever de indenizar. Preliminarmente, infere-se que o fato gerador de tal instituto é, justamente, o descumprimento obrigacional de cláusula contratual firmada ou, alternativamente, dever jurídico preexistente. Em suma, quanto à origem, existe a respectiva classificação em responsabilidade contratual e responsabilidade extracontratual ou aquiliana – foco da presente pesquisa. Nesse sentido, aquele que, por meio de suas atitudes, positivas ou negativas, viola direitos e, concomitantemente, provoca danos a outrem, comete ato ilícito e deve repará-lo. Segundo Flávio Tartuce (2015, p. 370):

> De início, o ato ilícito é o ato praticado em desacordo com a ordem jurídica, violando direitos e causando prejuízos a outrem. Diante da sua ocorrência, a norma jurídica cria o dever de reparar o dano, o que justifica o fato de ser o ato ilícito fonte do direito obrigacional. O ato ilícito é considerado como fato jurídico em sentido amplo, uma vez que produz efeitos jurídicos que não são desejados pelo agente, mas somente aqueles impostos pela lei.

Cavalieri Filho (2012, p. 3), por outro lado, adota a teoria de que "a responsabilidade é a sombra da obrigação", afinal, o dever jurídico inicialmente descumprido é tido como originário, sendo a necessidade de reparação um novo dever jurídico, de caráter sucessivo. Mediante, deve-se haver a prática antijurídica de atos, causadores de danos, para a concretização do dever de indenizar, previsto no regime de responsabilidade civil. Veja-se:

> Embora não seja comum nos autores, é importante distinguir a obrigação da responsabilidade. Obrigação é sempre um dever jurídico originário; responsabilidade é um dever jurídico sucessivo, consequente à violação do primeiro. Se alguém se compromete a prestar serviços profissionais a outrem, assume uma obrigação, um dever jurídico originário. Se não cumprir a obrigação (deixar de prestar os serviços), violará o dever jurídico originário, surgindo daí a responsabilidade, O dever de compor o prejuízo causado pelo não cumprimento da obrigação. Em síntese, em toda obrigação há um dever jurídico originário, enquanto que na responsabilidade há um dever jurídico sucessivo. Daí a feliz imagem de Larenz ao dizer que "a responsabilidade é a sombra da obrigação". Assim como não há sombra sem corpo físico, também não há responsabilidade sem a correspondente obrigação. (FILHO, 2012, p. 3).

Os Artigos 186, 187 e 927, todos do Código Civil Brasileiro (Lei nº 10.406/2002), formalizam:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Sinteticamente, é crível ressaltar que o ato ilícito, contrário às normas legais, corresponde a uma conduta humana voluntária, independentemente da existência de culpa (em sentido genérico), que traz prejuízos diretos a um indivíduo, gerando desequilíbrio social. Preceitua-se que o Código Civil de 2002 trouxe uma extensão à tal conceito, inserindo a prática

do abuso de direito como indevida e, se causadora de danos, passível de reparação. Portanto, as ações, omissões, negligência, imprudência e exercício irregular de direitos, quando provocam infortúnios, se enquadram no conceito de ato ilícito, tido como precursor da obrigação indenizatória. Nos dizeres de Caio Mário da Silva Pereira (2018, p. 28):

> A responsabilidade civil consiste na efetivação da reparabilidade abstrata do dano em relação a um sujeito passivo da relação jurídica que se forma. Reparação e sujeito passivo compõem o binômio da responsabilidade civil, que então se enuncia como o princípio que subordina a reparação à sua incidência na pessoa do causador do dano. Não importa se o fundamento é a culpa, ou se é independente desta. Em qualquer circunstância, onde houver a subordinação de um sujeito passivo à determinação de um dever de ressarcimento, aí estará a responsabilidade civil.

A partir da análise dos dispositivos legais, verifica-se que, apesar das divergências doutrinárias, a definição do instituto da responsabilidade civil mantém pressupostos gerais comuns. Entre eles, destacam-se: conduta humana, comissiva ou omissiva; ocorrência de um dano; nexo de causalidade entre a conduta e o prejuízo; e surgimento de um dever de reparação, voltado a restabelecer o equilíbrio rompido. Ademais, há o elemento subjetivo – culpa –, que pode ou não estar presente, dependendo da modalidade de responsabilidade, seja ela subjetiva ou objetiva (TARTUCE, 2015, p. 382), como será explorado.

1.1.1 Conduta humana

A conduta humana, tida como elemento inicial para a adequação dentro do regime de responsabilidade civil, "pode ser causada por uma ação (conduta positiva) ou omissão (conduta negativa) voluntária, ou por negligência, imprudência ou imperícia, modelos jurídicos que caracterizam o dolo e a culpa, respectivamente" (TARTUCE, 2015, p. 382). Nesse sentido, a ação deve ser fundamental para a concretização do dano, de modo que, sem ela, não se teria vislumbrado nenhum prejuízo.

Há uma evidente relação entre esse pressuposto e o conceito de "ato ilícito", vez que, em regra, a conduta humana voluntária deve conflitar com o ordenamento jurídico vigente, configurando, assim, um ato antijurídico. Contudo, ainda que de maneira excepcional, é possível que haja responsabilidade civil sem a presença de antijuridicidade, em virtude de normas legais específicas. Veja-se:

> Como já foi dito, em atenção ao estrito critério metodológico desta obra, preocupamo-nos em elencar os elementos realmente genéricos ou fundamentais da responsabilidade civil, características essas não existentes na característica da ilicitude. Sem ignorarmos que a antijuridicidade, como regra geral, acompanha a ação

> humana desencadeadora da responsabilidade, entendemos que a imposição do dever de indenizar poderá existir mesmo quando o sujeito atua licitamente. Em outras palavras: poderá haver responsabilidade civil sem necessariamente haver antijuridicidade, ainda que excepcionalmente, por força de norma legal. Por isso não se pode dizer que a ilicitude acompanha necessariamente a ação humana danosa ensejadora da responsabilização. (GAGLIANO; FILHO, 2012, p. 84)

Nesse contexto, é imprescindível que se faça um exame do modo como a ação, no caso concreto, feriu um ditame legal, ensejando prejuízos a outrem. Nas palavras de Cavalieri Filho (2012, p. 3): "sempre que quisermos saber quem é o responsável, teremos que identificar aquele a quem a lei imputou a obrigação, porque ninguém poderá ser responsabilizado por nada sem ter violado dever jurídico preexistente".

1.1.2 Culpa

O elemento "culpa", dentro do instituto da responsabilidade civil, deve ser analisado, à princípio, sob o ponto de vista genérico - *lato sensu* -, englobando o "dolo" e a "culpa em sentido estrito" – *stricto sensu*, de movo a facilitar sua identificação. Ressalta-se que é um pressuposto aplicado somente aos casos de responsabilidade subjetiva, onde o dever de reparação está atrelado à demonstração da conduta culposa, em moldes semelhantes à *Lex Aquilia*, citada alhures.

Primeiramente, o dolo revela a intenção deliberada do agente em adotar postura que fere uma obrigação primária, destacando a vontade livre e consciente de agir com o fim de prejudicar terceiros. Por sua vez, a culpa em sentido estrito indica que não se havia o interesse em violar dever jurídico preexistente, ou mesmo ensejar danos a outrem. Nas palavras de Cavalieri Filho (2012, p. 32):

> Tanto no dolo como na culpa há conduta voluntária do agente, só que no primeiro caso a conduta já nasce ilícita, porquanto a vontade se dirige à concretização de uni resultado antijurídico - o dolo abrange a conduta e o efeito lesivo dele resultante -, enquanto no segundo a conduta nasce lícita, tornando-se ilícita na medida em que se desvia dos padrões socialmente adequados. O juízo de desvalor no dolo incide sobre a conduta, ilícita desde a sua origem; na culpa, incide apenas sobre o resultado. Em suma, no dolo o agente quer a ação e o resultado, ao passo que na culpa ele só quer a ação, vindo a atingir o resultado por desvio acidental de conduta decorrente de falta de cuidado.

Segundo parcela doutrinária, há uma tendência, no estudo do Direito Contemporâneo, a entender a culpa como um erro ou desvio de conduta, afastando do conceito o estado de ânimo do agente. De acordo com Alvino Lima (1938, p. 41):

> Do que acabamos de expôr, verifica-se que o conceito de culpa, como elemento distinto e específico do ato ilícito, depende da fixação da conduta normal do homem adaptado à vida social, ao ambiente em que vive. Um êrro nesta conduta, um desvio dêste agir normal dos homens atendendo à situação em que se encontrará o autor do ato lesivo, determinará a sua responsabilidade extra-contratual, obrigando-o à reparação do dano causado, uma vez que os demais elementos do ato ilícito estejam comprovados. Em face, pois, de um fato concreto, violador do direito de outrém, uma vez verificados o dano e o laço de causalidade, surge, então, a indagação de se conhecer si o agente, ao praticar o ato, ao cometer a omissão, agiu, atendendo ás circunstâncias que o rodeavam, como todos nós agiríamos, como atuaria o homem prudente, normal, avisado. Si analisando a atitude do agente, aferindo-a por esta balança da conduta humana, em geral, verificarmos que não houve desvio do que comumente se faz, da maneira como geralmente se procede, não encontramos o elemento vivificador dos demais requisitos da responsabilidade; o ato deixará, consequentemente, de ser ilícito, embora lesivo do direito de outrem.

Portanto, o entendimento aproxima-se de uma visão mais objetiva da culpa (*lato sensu*), concentrando-se no desvio de conduta por parte do agente, em relação ao comportamento que seria esperado de uma pessoa em condições semelhantes. De toda forma, para o Direito Civil, "não importa se o Autor agiu com dolo ou culpa (em sentido estrito), vez que, a consequência inicial é a mesma: imputação do dever de reparação do dano, ou indenização dos prejuízos" (TARTUCE, 2015, p. 385). Atrelados a esse elemento estrutural, estão os conceitos de negligência - conduta omissiva - e imprudência - conduta comissiva -, trazidos no Artigo 186 do Código Civil.

Salienta-se, ademais, que, atualmente, embora o efeito da "culpa" seja o mesmo para "dolo" e "culpa em sentido estrito", os critérios para a fixação do ressarcimento são diferentes, observados os Artigos 944 e 945 do Código Civil, que dizem respeito à redução equitativa da indenização:

> Art. 944. A indenização mede-se pela extensão do dano.
> Parágrafo único. Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização.
>
> Art. 945. Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com a do autor do dano.

Como o critério para determinar o valor da indenização é baseado na extensão do dano causado, a análise da gravidade da culpa torna-se menos relevante, vez que, não há uma correspondência direta entre sua intensidade e o montante indenizatório. No entanto, conforme preceitua o Artigo 944 do Código Civil, que prevê a possibilidade de redução da indenização em caso de desproporção significativa entre o dano e a conduta do agente, a gravidade da culpa passa a ter um papel relevante.

1.1.3 Dano

O dano se mostra como um dos pilares de sustentação do instituto da responsabilidade civil, afinal, é terminantemente impossível imputar obrigação indenizatória sem que a conduta tenha, efetivamente, causado prejuízos. Nesse sentido, deve-se verificar lesão a um bem jurídico tutelado, de modo a trazer consequências efetivas a terceiros. Nas palavras de Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 90 -92), existem requisitos a serem observados para que o dano seja indenizável, a saber: "violação de um interesse jurídico patrimonial ou extrapatrimonial de uma pessoa física ou jurídica; certeza do dano e subsistência do dano". Em suma, a quebra do equilíbrio social deve explicitar a efetiva perda que uma pessoa teve, em detrimento das atitudes de outra, sendo a indenização um meio de compensação do transtorno.

Destaca-se que o dano pode ter caráter patrimonial (ou material) e moral, a depender de sua extensão no caso concreto. O primeiro deles diz respeito à lesão aos bens e direitos economicamente apreciáveis de seu titular, subdividindo-se em danos emergentes – redução efetiva do patrimônio da vítima – e lucros cessantes – correspondentes àquilo que a vítima, razoavelmente, deixou de lucrar, por força do dano. Veja-se:

> Os danos patrimoniais ou materiais constituem prejuízos ou perdas que atingem o patrimônio corpóreo de alguém. Pelo que consta dos arts. 186 e 403 do Código Civil não cabe reparação de dano hipotético ou eventual, necessitando tais danos de prova efetiva, em regra. Nos termos do art. 402 do CC, os danos materiais podem ser assim subclassificados: Danos emergentes ou danos positivos – o que efetivamente se perdeu. Como exemplo típico, pode ser citado o estrago do automóvel, no caso de um acidente de trânsito. Como outro exemplo, a regra do art. 948, I, do CC, para os casos de homicídio, devendo os familiares da vítima ser reembolsados pelo pagamento das despesas com o tratamento do morto, seu funeral e o luto da família. Lucros cessantes ou danos negativos – o que razoavelmente se deixou de lucrar. No caso de acidente de trânsito, poderá pleitear lucros cessantes o taxista, que deixou de receber valores com tal evento, fazendo-se o cálculo dos lucros cessantes de acordo com a tabela fornecida pelo sindicato da classe e o tempo de impossibilidade de trabalho (TJSP, Apelação Cível 1.001.485-0/2, São Paulo, 35.ª Câmara de Direito Privado, Rel. Artur Marques, 28.08.2006, v.u., Voto 11.954). Como outro exemplo de lucros cessantes, cite-se, no caso de homicídio, a prestação dos alimentos indenizatórios, ressarcitórios ou indenitários, devidos à família do falecido, mencionada no art. 948, II, do CC. (TARTUCE, 2015, p. 394-395)

Quanto aos danos morais, diversos são os conceitos abarcados pela doutrina e jurisprudência. Para fins da presente pesquisa, será adotada a definição trazida por Cavalieri Filho (2012, p. 90-91):

> Como se vê, hoje o dano moral não mais se restringe à dor, tristeza e sofrimento, estendendo a sua tutela a todos os bens personalíssimos - os complexos de ordem ética -, razão pela qual podemos defini-lo, de forma abrangente, como sendo uma agressão

> a um bem ou atributo da personalidade. Em razão de sua natureza imaterial, o dano moral é insusceptível de avaliação pecuniária, podendo apenas ser compensado com a obrigação pecuniária imposta ao causador do dano, sendo esta mais uma satisfação do que uma indenização.

Denota-se que os danos morais dizem respeito à violação de direitos inerentes à condição humana, sendo inadequado reduzi-los, meramente, a uma quantificação monetária. Portanto, além de desempenharem função punitiva em relação ao ofensor, buscam, dentro dos limites aplicáveis, compensar o sofrimento experimentado pela vítima, mesmo que não seja possível restabelecer, plenamente, o *status quo ante*.

Ademais, relevante destacar que existem danos afetos à coletividade, atacáveis por meio de ações coletivas. Segundo previsão do Artigo 81 da Lei nº 8.078/1990 (Código de Defesa do Consumidor), a defesa coletiva será exercida quando se tratar de interesses ou direitos difusos; interesses ou direitos coletivos, e interesses ou direitos individuais homogêneos. O critério a ser considerado é, precisamente, "o direito subjetivo específico que foi violado", segundo entendimento de Antonio Gidi *apud* Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 99).

1.1.4 Nexo de causalidade

Para a incidência do dever de indenizar, é necessário que exista uma relação direta de causa e consequência entre a conduta culposa, ou o risco criado, e o infortúnio trazido a terceiros. Nesse sentido, o nexo causal une as extremidades da ação – atitude voluntária - e reação – dano -, funcionando como um cano virtual (TARTUCE, 2015, p. 388). Concomitantemente, o ato antijurídico, advindo da conduta humana voluntária, está obrigado a desencadear prejuízos diretos, se adequando, assim, ao instituto da responsabilidade civil. Nas palavras de Cavalieri Filho (2012, p. 49):

> Não basta, portanto, que o agente tenha praticado uma conduta ilícita; tampouco que a vítima tenha sofrido um dano. E preciso que esse dano tenha sido causado pela conduta ilícita do agente, que exista entre ambos uma necessária relação de causa e efeito. Em síntese, é necessário que o ato ilícito seja a causa do dano, que o prejuízo sofrido pela vítima seja resultado desse ato, sem o que a responsabilidade não correrá a cargo do autor material do fato. Daí a relevância do chamado nexo causal. Cuida-se, então, de saber quando um determinado resultado é imputável ao agente; que relação deve existir entre o dano e o fato para que este, sob a ótica do Direito, possa ser considerado causa daquele.

Outrossim, à luz dos ensinamentos de Flávio Tartuce (2015), o Código Civil de 2002 destaca duas teorias fundamentais: a teoria da causalidade adequada, que busca identificar a

causa que, de maneira potencial, foi determinante para a ocorrência do dano; e a teoria do dano direto e imediato (também conhecida como teoria da interrupção do nexo causal), que estabelece que apenas os prejuízos decorrentes, necessariamente, da conduta do agente devem ser reparados. Portanto, incumbe ao jurista, analisando o caso concreto, aplicar a doutrina que melhor se adeque às especificidades da situação, observados os princípios jurídicos pertinentes, os fatos expostos e a jurisprudência consolidada.

Infere-se que, entre as causas excludentes do dever de indenizar, enquadram-se aquelas relativas à ruptura do nexo causal, a saber: caso fortuito e força maior. Com base nos ensinamentos de Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 182), a força maior ocorre quando um evento inevitável se concretiza, mesmo sendo conhecido, a exemplo de um terremoto previsto por cientistas, mas impossível de evitar. Já o caso fortuito envolve uma situação inesperada, que surpreende, como um acidente ou roubo. Nessa circunstância, a imprevisibilidade afeta a parte incauta, impossibilitando o cumprimento de uma obrigação.

Por fim, convém destacar a inequívoca distinção na caracterização do vínculo causal das modalidades de responsabilidade subjetiva e objetiva. Na primeira, este é delineado pela culpa em sentido amplo (*lato sensu*) – abarcando o dolo e a culpa *stricto sensu* -, como preceitua o Artigo 186 do Código Civil. Na segunda, o nexo causal se configura a partir da mera conduta, aliada à previsão legal de responsabilização independentemente de culpa, ou em razão da atividade de risco, nos termos do Artigo 927, parágrafo único, do Código Civil (TARTUCE, 2015, p. 388-389).

1.2 Modalidades de Responsabilidade Civil: Subjetiva e Objetiva

As modalidades constantes no regime de responsabilidade civil são classificadas em subjetiva e objetiva, sendo a distinção substancial entre elas relativa à presença do elemento "culpa", exposto alhures.

Observa-se que o primeiro modelo representa a regra geral do ordenamento jurídico brasileiro. Para sua incidência, inelutável demonstrar a intenção do agente em causar o dano (dolo) ou, alternativamente, comprovar que este agiu com negligência, imprudência ou imperícia (culpa em sentido estrito), conforme inteligência do Artigo 186 do Código Civil. Embora padeça do elemento introspectivo, pode ser aplicado na ausência de prova direta do prejuízo. Em determinadas circunstâncias, este é considerado presumido, consoante a teoria do dano *in re ipsa*, que dispensa a necessidade de comprovação expressa do resultado lesivo, vez que deriva, naturalmente, do próprio ato ilícito (TARTUCE, 2015, p. 419). Portanto, a

responsabilização pode ocorrer sem a necessidade de demonstrar o dano objetivamente, desde que a conduta e o nexo causal estejam claramente definidos.

Em contrapartida, o segundo modelo ressalta a existência de uma exceção legal relevante. A análise do Artigo 927, parágrafo único, do Código Civil, permite concluir que a obrigação indenizatória subsiste, independentemente de comportamento culposo, nos casos expressamente previstos no ordenamento jurídico, ou quando a atividade desenvolvida pelo causador do infortúnio, por sua própria natureza, gera um risco inerente aos direitos de terceiros. Nesse contexto, são delineadas duas abordagens principais: uma baseada na teoria do risco, em que a responsabilidade decorre, simplesmente, da possibilidade de dano, e outra concernente aos casos especificados legalmente, nos quais a indenização é imposta como uma consequência objetiva da atividade (TARTUCE, 2015, p. 420).

No Brasil, a teoria do risco não dispõe de doutrina unificada, afinal, o texto legal abre margem para ampla interpretação, especialmente por parte do jurista, em um caso concreto. Nas palavras de Cavalieri Filho (2012, p. 152): "Risco é perigo, é probabilidade de dano, importando, isso, dizer que aquele que exerce uma atividade perigosa deve-lhe assumir os riscos e reparar o dano dela decorrente". Mediante, configura-se quando a função do agente causador impõe ônus superior ao suportado pelos demais membros da coletividade. Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 217) lecionam:

> No nosso entendimento, ao consignar o advérbio "normalmente", o legislador quis referir-se a todos os agentes que, em troca de determinado proveito, exerçam com regularidade atividade potencialmente nociva ou danosa aos direitos de terceiros. Somente essas pessoas, pois, empreenderiam a mencionada atividade de risco, apta a justificar a sua responsabilidade objetiva. Note-se, inclusive, que não se exige que a conduta lesionante seja ilícita *stricto sensu*, mas, sim, pelo fato de que seu exercício habitual pode, potencialmente, gerar danos a outrem, não sendo razoável admitir-se que a autorização legal para o exercício de uma atividade importe em considerar lícita a lesão a direito de terceiros.

A priori , sob a ótica de Flávio Tartuce (2015, p. 419-420), destacam-se cinco teorias majoritariamente aplicadas na jurisprudência. A primeira delas, "Teoria do risco administrativo", responsabiliza o Estado por prejuízos emanados a terceiros (Artigo 37, § 6º, da CRFB/88). A "Teoria do risco criado" incumbe ao agente os riscos advindos de suas ações, ainda que involuntárias (Artigo 938 do Código Civil). Já a "Teoria do risco da atividade" impõe responsabilidade objetiva em tarefas que, por sua condição inerente, são arriscadas (Artigo 927, parágrafo único, do Código Civil). A "Teoria do risco-proveito" estabelece que o beneficiário de atividade lucrativa deve assumir os riscos envolvidos, especialmente nas relações de consumo (Enunciado n. 43 do CJF/STJ). Por fim, a "Teoria do risco integral" suprime

excludentes de responsabilidade em casos específicos, como os relacionados a danos ambientais (Artigo 14, § 1º, da Lei nº 6.938/1981).

À posteriori, existem os cenários jurídicos que preveem, especificamente, a responsabilização sem culpa. É o caso do Código de Defesa do Consumidor (Lei nº 8.078/1990), que impõe aos fornecedores de produtos ou serviços a obrigação de indenizar os consumidores pelos prejuízos causados. Nesse ponto, destacam-se os conceitos trazidos pelos Artigos 2º e 3º do CDC:

> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.
> Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.
>
> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

Para o alinhamento junto ao modelo objetivo, a relação de consumo deve integrar, inequivocamente, as figuras do consumidor e fornecedor, nos termos da legislação vigente. De mais a mais, imperioso clarificar que, consoante entendimento pacificado dos Tribunais Superiores, a redação do Artigo 3º, § 2º, deve ser extensa, abarcando, também, a remuneração indireta, consubstanciada no proveito econômico dos fornecedores de serviços gratuitos, a exemplo do TikTok (aplicativo de compartilhamento de vídeos). Veja-se:

> CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA VOLTADA AO COMÉRCIO ELETRÔNICO. INTERMEDIAÇÃO. AUSÊNCIA. FORNECEDOR. NÃO CONFIGURADO. [...] 2. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. 3. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo. 4. Existência de múltiplas formas de atuação no comércio eletrônico. [...] (REsp 144008/RS, Rel. Min. Nancy Andrighi, TERCEIRA TURMA, Julgado em 25/10/2016. DJe 09/11/2016). "2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração', contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor." (STJ - REsp: 1316921 RJ 2011/0307909-6, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 26/06/2012, T3 - TERCEIRA TURMA, Data de Publicação: DJe 29/06/2012)

Sob essa conjuntura, Cavalieri Filho (2012, p. 515-517) postula a existência de princípios norteadores, a serem aplicados nas articulações consumeristas. Entre eles, estão: reparação completa por prejuízos materiais e morais (Artigo 6º, VI, do CDC); proibição de cláusulas que restrinjam ou excluam o direito à compensação (Artigo 51, IV e §1º, do CDC; medidas preventivas para impedir a ocorrência de novos prejuízos (Artigo 6º, VI, do CDC); necessidade de disponibilizar informações de maneira clara, objetiva e ostensiva (Artigos 6º, III, e 31 do CDC); e incumbência de assegurar que somente produtos e serviços confiáveis sejam oferecidos à coletividade (Artigo 8º do CDC).

Por conseguinte, a inobservância aos mandamentos legais enseja a obrigação indenizatória, que independe, em regra, da existência de culpa *lato sensu*. Assim, em situações envolvendo fatos do produto – ou seja, defeitos no produto fornecido ao consumidor -, aplica-se a regra prevista no Artigo 12 do CDC. Diversamente, nos casos relativos a fatos do serviço – defeitos na prestação de serviços -, segue-se a disciplina constante no Artigo 14 do CDC, que merece enfoque, para fins do presente trabalho:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido.
> § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.
> § 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.

Denota-se que o fornecedor de serviços poderá eximir-se, unicamente, provando uma das hipóteses dispostas no §3º do dispositivo retro. Concomitantemente, tal norma é substancial para a proteção das relações de consumo, vez que, a adoção da modalidade objetiva de responsabilização culmina por fortalecer o sistema de defesa do consumidor. Carlos Eduardo Pianovski Ruzyk *apud* Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2012, p. 386) elucida: "A operacionalização desse instituto pode produzir uma intervenção na relação meios-fins da atividade econômica, tornando ineficiente aquilo que pode violar o princípio da dignidade. Trata-se de tornar ineficiente aquilo que já é antijurídico".

Indiscutivelmente, a aplicação do referido regime está intrinsicamente ligada aos prejuízos decorrentes do uso de mecanismos de inteligência artificial, cuja adoção crescente no mercado, em face da falta de regulamentação específica no direito brasileiro, cria lacunas legais relevantes. Por isso, como se verá, muitos estudiosos consideram a abordagem adequada, vez que permite a responsabilização direta, sem a necessidade de comprovação de culpa. Dessa forma, a teoria objetiva surge como uma solução alternativa para lidar com questões como violações de privacidade e falhas na coleta e tratamento de dados pessoais, áreas em que as IA´s têm impactos profundos e difíceis de controlar.

1.3 Responsabilidade Civil no Contexto de Novas Tecnologias

A responsabilidade civil, no contexto das inovações contemporâneas, assume papel potencialmente desafiador, afinal, são notórios os avanços no âmbito das interações entre seres humanos e novas tecnologias. Atualmente, discute-se a chamada 4ª Revolução Industrial, que inclui mecanismos controlados autonomamente, dos quais derivam as "inteligências artificiais" (FARIA; DAMASCENO, 2019, p. 239-261). Sucintamente, as IA´s, segundo Paulo Sá Elias (2019, p. 1-2), dizem respeito ao desenvolvimento de sistemas de computadores capazes de executar tarefas que, normalmente, exigiriam a inteligência humana. Isso ocorre, por exemplo, quando estes, a partir das informações coletadas, tomam decisões em diferentes áreas do conhecimento, substituindo, em parte, a força motriz humana.

Conforme exposto pelo Conselho Nacional de Justiça (CNJ), há uma divisão entre dois tipos de IA: a Inteligência Artificial Geral, também chamada de "IA forte", e a "IA fraca". Atualmente, difunde-se, especialmente, a versão "fraca", por meio da qual são projetados resultados significativos no processamento de dados, e na respectiva conversão em soluções estratégicas para as organizações. A configuração "forte", até o momento, fomenta discussões majoritariamente teóricas, embasando uma corrente de pensamento que acredita na possibilidade de consolidação de máquinas capazes de pensar, criar, raciocinar e ter consciência própria, como preceitua Amanda Lemos (2022, s.p.).

Sob essa ótica, destacam-se duas possíveis formas de aprendizado: *machine learning* e *deep learning.* A primeira delas - aprendizado da máquina - envolve o treinamento de algoritmos para que identifiquem padrões e façam previsões a partir de dados, melhorando o desempenho de uma função, através da experiência, e propiciando a aprendizagem de maneira independente (ELIAS, 2019, p. 2). O segundo modelo – aprendizado profundo - , por sua vez, possui estrutura mais complexa que, inspirada no cérebro humano, promove a evolução de

“redes neurais artificiais”, nas quais cada camada (*layer*) escolhe um recurso específico para absorver (ELIAS, 2019, p. 2). Assim, à medida em que o sistema recebe informações, a capacidade de retenção e a aptidão para desempenhar tarefas aumentam progressivamente.

Em abordagem unificada, trazida por Isaías Lima (2014, p. 4), o desafio desses algoritmos é aprimorar a capacidade de generalizar o que aprenderam, desenvolvendo a habilidade para que uma máquina responda, de forma eficaz, a novos conjuntos de dados. Os sistemas precisam identificar, satisfatoriamente, as relações entre as variáveis envolvidas (entrada e saída), a partir das informações colacionadas. Com base nos ensinamentos de Pedro Domingos (2017, p. 30):

> Os algoritmos de aprendizado são os conciliadores: eles unem produtores e consumidores, rompendo a sobrecarga de informações. Se forem suficientemente inteligentes, você terá o melhor de dois mundos: a ampla gama de opções e o baixo custo da larga escala com o toque personalizado da pequena escala. Os aprendizes não são perfeitos, e geralmente a última etapa da decisão continua sendo uma tarefa para os humanos, mas eles reduzem de maneira inteligente as opções a algo que uma pessoa possa gerenciar.

O TikTok, na prática, exemplifica o exposto alhures, afinal, as informações coletadas por sua Inteligência Artificial buscam estabelecer uma relação entre o comportamento do usuário e os tipos de vídeos que devem ser recomendados para mantê-lo engajado. Em suma, quanto mais detalhes o algoritmo recebe acerca da conduta adotada, melhor se torna em prever e recomendar conteúdos que têm mais chances de serem apreciados por aquela pessoa. Nesta conjuntura, casos de armazenamento e processamento inadequados de dados levantam uma questão extremamente pertinente: a quem atribuir o dever da responsabilidade civil, considerando os elementos estruturais definidos pela legislação brasileira.

A priori , destaca-se a influência do ordenamento jurídico europeu no desenvolvimento de disposições atinentes às novas tecnologias. É sabido que, em abril de 2021, a União Europeia publicou esboço da regulação das inteligências artificiais, clarificando a proteção enfática do cidadão europeu em áreas como saúde, segurança e direitos fundamentais (ZIMPRICH, 2021). Com a evolução contínua das IA´s, o Parlamento Europeu consolidou o referido esboço, dando origem, em junho de 2023, à primeira legislação de inteligência artificial do mundo, a ser integrada, paulatinamente, até o ano de 2026.

Consoante o próprio Parlamento, devem ser observados requisitos específicos, visando à transparência; proteção de direitos solidificados, segurança dos sistemas e prevenção de danos. Neste caminhar, foram pormenorizados os sistemas de risco elevado (gestão de infraestruturas essenciais, educação, saúde, aplicação da lei, entre outros), que serão avaliados

antes de serem inseridos no mercado e durante todo o seu ciclo de existência, imputando-se, objetivamente, a obrigação de reparação por eventuais prejuízos.

O Brasil, por sua vez, não dispõe de regulamentação jurídica específica. Em verdade, temos, sob influência das discussões fomentadas, especialmente, pela União Europeia, 46 projetos de lei em tramitação no Congresso Nacional. Um dos mais emblemáticos e criticados, o Projeto de Lei 21/2020, que tramita perante a Câmara dos Deputados, assegura "princípios, direitos, deveres e instrumentos de governança para o uso da inteligência artificial", determinando "diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios, pessoas físicas e jurídicas, de direito público ou privado, e entes sem personalidade jurídica em relação à matéria". Contudo, adota a modalidade subjetiva de responsabilidade civil, o que não parece harmonizar com o entendimento legal. Segundo o professor Anderson Schreiber:

> […] não faz sentido que um projeto de lei sobre IA contenha um dispositivo que prevê que as normas sobre responsabilidade civil dos agentes que atuam no desenvolvimento e operação dos sistemas de IA devam se pautar pela responsabilidade civil subjetiva. Em primeiro lugar, não faz muito sentido que uma lei ordinária crie uma norma dizendo que há preferência por um certo regime de responsabilidade civil, porque uma lei ordinária posterior naturalmente teria que especificar, concretizar essa preferência – isso tornaria o dispositivo anterior totalmente desnecessário. Segundo, se houvesse alguma preferência dentro do ordenamento brasileiro, (…) de acordo com a nossa doutrina, com a nossa jurisprudência, inclusive o Código Civil, de que a preferência seria pela responsabilidade civil objetiva (…). A legislação consumerista também adota o regime de responsabilidade objetiva, embora com algumas peculiaridades, de maneira que a introdução de uma nova tecnologia, como é a IA, sem dúvida alguma, se enquadraria dentro desse conjunto de hipóteses e atrairia, dentro do nosso sistema jurídico, a responsabilidade civil objetiva. (SENADO FEDERAL, 2022, p. 93)

Nelson Rosenvald também aponta que a seleção simplificada da responsabilidade subjetiva, enquanto regime único, contradiz a própria complexidade do que se pretende regular (SENADO FEDERAL, 2022, p. 95). Mediante, em resposta às falhas, fora desenvolvido, entre outros, o PL 2338/2023, junto ao Senado Federal. Este prevê, semelhantemente aos moldes europeus, normas gerais para a formação, implementação e uso responsável de sistemas inteligentes, com o fito de "proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico". Ademais, adota, via de regra, o modelo objetivo de responsabilização.

Infere-se que as propostas estão em construção, não tendo sido integradas ao ordenamento jurídico brasileiro. Por tal motivo, a problemática será analisada, inicialmente,

com base nas normativas vigentes. Assim, segundo parcela doutrinária, os pressupostos da responsabilidade civil devem ser ressignificados, conjecturando que o ineditismo das questões suscitadas pelas novas tecnologias não corresponde, necessariamente, ao ineditismo das soluções jurídicas. Note-se:

> Conforme ressaltado, não parece aconselhável o abandono das formulações desenvolvidas historicamente para a conformação da responsabilidade civil tal como hoje conhecida. Se é verdade que as novas tecnologias impõem renovados desafios, o direito civil mostra-se apto a oferecer as respostas adequadas a partir de seus próprios fundamentos teóricos. Oxalá possa o encanto pelas novas discussões envolvendo robôs e sistemas autônomos atuar como subsídio para a sempre necessária renovação do interesse no aperfeiçoamento dos estudos sobre a responsabilidade civil, sem que se recorra, mediante o atalho mais fácil – embora por vezes desastroso – ao anúncio de novos paradigmas que, descomprometidos com o sistema, justifiquem soluções casuísticas, em constrangedora incompatibilidade com a segurança jurídica oferecida pela dogmática do direito civil na legalidade constitucional. (TEPEDINO; SILVA, 2019, p. 85-86).

Concomitantemente, adequando o fato à norma, percebemos que a coleta indevida de dados, especialmente informações pessoais sensíveis, embora realizada por meio dos mecanismos de aprendizagem da IA, gera danos evidentes, consolidando o "prejuízo" como um dos pilares do Instituto da Responsabilidade Civil. Todavia, a latente complexificação desses sistemas dificulta o reconhecimento dos demais elementos, como a conduta humana derivada de ato ilícito, a culpa - a depender do regime de responsabilidade aplicado - e o nexo de causalidade, tornando-os menos evidentes.

Em um primeiro momento, paira-se a dúvida acerca do agente responsável pelo infortúnio, vez que, a inteligência artificial não é dotada de personalidade jurídica. Com base nos ensinamentos de Gustavo Tepedino e Rodrigo da Guia Silva (2019, p. 79), “toda a investigação da imputabilidade do dever de indenizar gira em torno da atribuição de responsabilidade a pessoas, e não a robôs”. Nesse cenário, imprescindível analisar o vínculo entre o operador do sistema e o dano provocado, levando em consideração, inclusive, o grau de intervenção do usuário (TEPEDINO; SILVA, 2019, p. 79). Sinteticamente, a obrigação indenizatória recairá sobre o indivíduo que exercia controle e supervisão sobre a IA, sendo ele o encarregado pela operação e pelos efeitos resultantes do seu funcionamento.

À luz do ordenamento jurídico brasileiro, identificam-se legislações complementares que regulam o tratamento de dados, delineando os potenciais responsáveis em casos de irregularidades, seja nas relações de consumo ou em outros cenários. O Código de Defesa do Consumidor (CDC), a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet (MCI) estabelecem diretrizes claras acerca da conduta exigida, e as respectivas sanções

aplicáveis aos desvios. Mediante, oferecem uma base jurídica para a responsabilização, ainda que não abarquem, diretamente, as particularidades envolvidas no uso dos sistemas inteligentes.

Dessa forma, inelutável aprofundar o estudo quanto à utilização de dados e a imputação de responsabilidades pelos prejuízos advindos de falhas, sobretudo em situações de coleta indevida de informações, considerando não apenas o Código Civil, mas também as normativas correlatas. Ratifica-se que, embora o dano seja explícito, imperioso delimitar, com rigor analítico, os elementos mais nebulosos, também destacados nas referidas leis complementares.

CAPÍTULO 2 - REGULAÇÃO DA COLETA DE DADOS PESSOAIS NO BRASIL

Como demonstrado alhures, os avanços tecnológicos contínuos suscitaram questões antes inexploradas. A criação de sistemas inteligentes, que utilizam a coleta de dados para traçar perfis comportamentais e oferecer soluções otimizadas, gerando, especialmente, benefícios financeiros para empresas, é um exemplo significativo, embora não seja o único. Paralelamente, relevante examinar a trajetória histórica da coleta de dados pessoais, no Brasil, enfatizando a evolução dos conceitos e aplicações, até a estruturação atualmente conhecida. O estudo é fundamental para assegurar que as inteligências artificiais, dependentes do armazenamento de informações, operem em concordância com a legislação vigente, permitindo a responsabilização apropriada, em cenários de danos por descumprimento das normas jurídicas.

A priori , clarifica-se que o conceito de dados pessoais está intrinsecamente vinculado ao direito à privacidade, sendo entendido como uma extensão deste, consoante os ensinamentos de Danilo Ricardo Ferreira Barbosa e Carlos Sérgio Gurgel da Silva (2019, p. 478). Nesse ponto, paira-se a dúvida relativa ao significado da terminologia, que sofreu bruscas alterações ao longo dos anos. Suas primeiras manifestações, ainda incipientes, foram observadas na Carta Magna de 1891 que, ao salvaguardar a inviolabilidade do sigilo de correspondências (Artigo 72, § 18), introduziu a garantia, ao indivíduo, de controlar suas próprias informações. Ressalta-se que as Constituições de 1934 (Artigo 113, § 8º) e 1946 (Artigo 141, § 6º) conservaram o amparo legal, que fora revisado posteriormente.

Mediante, após a Segunda Guerra Mundial (1939-1945), a Declaração Universal dos Direitos Humanos (1948) fortaleceu a proteção à vida privada, consagrando, em seu Artigo 12, que: “Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques”. A legislação brasileira, influenciada, incorporou o referido texto, a partir da promulgação da Constituição de 1967, que, além de garantir a inviolabilidade das correspondências, estendeu a tutela ao sigilo das comunicações telegráficas e telefônicas (Artigo 150, § 9º).

Contudo, apesar das inequívocas melhorias, a noção de privacidade se consolidou, efetivamente, com a Constituição de 1988. Esta, em seu Artigo 5º, incisos X e XII, conjectura:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> [...]

A análise do inciso X explicita uma proteção abrangente e específica de novos aspectos, como a intimidade - melhor detalhada no inciso XII - e a vida privada, que, de modo geral, fazem parte da composição do direito à privacidade. Para Tércio Sampaio Ferraz Junior (1993, v. 88, p. 439-459), a intimidade se encontra no núcleo essencial de cada indivíduo, em um campo exclusivamente pessoal e reservado. Em contrapartida, a vida privada está mais ligada ao cotidiano das pessoas e suas interações sociais. Concisamente, ambos se fundem como privacidade, englobando, também, a honra e a imagem das pessoas.

Para fins práticos, embora não haja um entendimento doutrinário ou legislativo uniformizado, a explanação proposta por Marcel Leonardi busca oferecer uma objetividade mínima ao delinear a privacidade como a capacidade do indivíduo de controlar a circulação de informações sobre si, reunindo e citando, em sua obra, as definições de Pereira, Hughes e Kuhlen para ampliar a compreensão enquanto:

> [...] o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito". A privacidade é, assim, "o poder de revelar-se seletivamente ao mundo" e não significa apenas o direito de ser deixado em paz, mas também "o direito de determinar quais atributos de si serão usados por outros (LEONARDI, 2011, p. 402).

Indubitavelmente, a Constituição de 1988 elevou a proteção à privacidade a um novo patamar, impondo sanções aos que a desrespeitarem. Contudo, com o avanço massivo das tecnologias de comunicação e o intenso fluxo de informações, especialmente na esfera digital, a tutela constitucional mostrou-se insuficiente, afinal, todos passaram a ser suscetíveis à exposição desautorizada de sua vida privada.

Nesse contexto, o Código de Defesa do Consumidor (CDC) trouxe a primeira referência aos "dados pessoais", apontando a necessidade de regulamentações mais específicas. Na sequência, o Marco Civil da Internet estabeleceu diretrizes para o uso responsável da internet, e a Lei Geral de Proteção de Dados (LGPD) consolidou normas abrangentes para a coleta e tratamento dos dados. Portanto, torna-se indispensável examinar como cada legislação

contribui para a proteção desse aspecto do direito à privacidade, destacando as possíveis formas de responsabilização em casos de violação e prejuízos decorrentes.

2.1 Conceito e Princípios Basilares da Coleta e Tratamento de Dados Pessoais

A evolução do termo "dados pessoais", no ordenamento jurídico brasileiro, explicita uma resposta gradual às inovações tecnológicas e à complexidade crescente dos métodos de coleta e tratamento de informações. A terminologia, que se configura como uma extensão do direito à privacidade, foi inicialmente delineada pelo Código de Defesa do Consumidor (Lei nº 8.078/1990). Este, em seu Artigo 43, celebra a proteção dos dados no contexto das relações consumeristas, ainda que sem defini-los de modo explícito. Posteriormente, a Lei de Acesso à Informação (Lei nº 12.527/2011) avança ao caracterizar "informação pessoal" como qualquer dado relacionado a uma pessoa natural identificada ou identificável (Artigo 4º, IV), estabelecendo, por analogia, uma base para o conceito de "dado pessoal". Veja-se:

> Art. 4º Para os efeitos desta Lei, considera-se:
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> [...]
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
> [...]

Todavia, Danilo Doneda (2011, p. 94) ratifica a distinção substancial entre “dado” e “informação”, afinal, enquanto o primeiro diz respeito à unidade bruta e isolada, o segundo é marcado pelo dado interpretado e contextualizado, que incorpora significado. Observa-se, ainda, que o Marco Civil da Internet (Lei nº 12.965/2014), embora tenha adotado a proteção de dados pessoais como um de seus princípios fundantes (Artigo 3º, III), não consolidou uma definição clara e objetiva para o termo, perpetuando as lacunas interpretativas.

Nesse ponto, é crível inferir que o desenvolvimento de legislações de proteção de dados, especialmente após a criação da primeira lei, em 1970, na Alemanha, motivou o Brasil a buscar alinhamento com os padrões internacionais. A exigência se intensificou em 2005, quando a Argentina, que já dispunha de normativa correlata, incentivou a criação de um dispositivo semelhante, visando à harmonização das regras dentro do Mercosul. A carência de norma específica dificultava a atração de investimentos estrangeiros e limitava o fluxo de dados com a União Europeia (UE), que prevê um “nível adequado” de proteção para transferências de informações pessoais (REINALDO FILHO, 2018).

Mediante, a sanção da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), pouco após a entrada em vigor da *General Data Protection Regulation* (GDPR) - legislação atualizada e unificada de proteção de dados e leis de privacidade -, na UE, representa a resposta brasileira às expectativas do mercado globalizado. Até então, o ordenamento jurídico não havia sido eficaz na definição inequívoca de "dados pessoais" e, tampouco, acompanhava as transformações tecnológicas e regulatórias em curso, no que tange à sua coleta, uso e tratamento. Com a LGPD, estabeleceu-se, formalmente, que:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais

> que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A partir do referido marco, houve a divisão dos dados pessoais em duas categorias majoritárias: dados identificadores e dados identificáveis. Os dados identificadores aludem a elementos como nome, CPF, RG e fotografia, capazes de diferenciar, especificamente, o indivíduo. Por sua vez, os dados identificáveis, embora não permitam a identificação direta, possibilitam individualizar a pessoa, ao serem combinados com outras informações. Também se incluem os dados anonimizados, que, à princípio, não estão ligados a nenhuma identidade, mas podem, em determinados cenários, tornar-se identificáveis.

Sob essa perspectiva, a Teoria do Mosaico, explicada por Fulgencio Madrid Conesa (1984, p. 45, *apud* OLIVEIRA, 2017, p. 66), sustenta que, assim como pequenas peças formam uma imagem completa em um mosaico, informações dispersas ganham sentido e se tornam identificáveis, ao serem organizadas de forma coesa. Cristiana Campos Mamede Maia (2019) ilustra que uma placa de carro, por exemplo, pode não ser um dado pessoal, se considerada isoladamente. Porém, ao ser cruzada com dados de inadimplência no IPVA e outros registros públicos, permite identificar o titular, revelando informações detalhadas sobre sua vida privada, sem uma invasão direta à intimidade.

Plataformas como Spotify, Netflix e TikTok elucidam o fenômeno, ao cruzar múltiplos dados para oferecer sugestões que se ajustam, precisamente, ao gosto individual do usuário. Em suma, os sistemas de recomendação inteligente adotam algoritmos sofisticados que, com base em vastas redes de dados pessoais, conseguem antecipar as preferências dos usuários, de forma quase preditiva. Segundo a doutrina de Danilo Ricardo Ferreira Barbosa e Carlos Sérgio Gurgel da Silva (2019, p. 496), o mecanismo não só intensifica a personalização, mas também aprofunda a coleta de informações, ampliando o grau de detalhamento dos perfis gerados e consolidando o uso estratégico de dados, para finalidades comerciais.

Portanto, mister se faz a observância à legislação vigente, que estipula fundamentos e princípios norteadores para as atividades de manuseio de dados pessoais. Inicialmente, à luz do Artigo 2º da LGPD, a temática deve ser regida pelo respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; desenvolvimento econômico e

tecnológico e inovação; livre iniciativa, livre concorrência e defesa do consumidor; e direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

Por outro lado, o Artigo 6º apresenta 10 (dez) diretrizes basilares que orientam o tratamento de dados pessoais, assegurando que este seja realizado com respeito à boa-fé e à proteção dos direitos dos titulares. O princípio da finalidade delimita que o processamento deve restringir-se, exclusivamente, ao objetivo informado no momento da coleta, impedindo o uso posterior para propósitos incompatíveis ou irrestritos. A adequação estipula o manuseio condizente com as finalidades comunicadas, coibindo arbitrariedades; enquanto a necessidade cerceia a manipulação dos dados ao indispensável para a concretização da atividade. O princípio do livre acesso assegura o direito de acesso às informações individuais, de modo facilitado e gratuito. Por sua vez, a qualidade dos dados garante que os registros sejam exatos, claros e atualizados, tendo por base a razão para a qual foram coletados.

Adiante, a transparência emerge como um dos pilares mais relevantes, ao formalizar que os titulares sejam plenamente informados sobre o uso de seus dados, evidenciando clareza e acessibilidade em todas as etapas do tratamento. A segurança exige a implementação de medidas técnicas e administrativas eficazes, para resguardar os dados pessoais contra acessos não autorizados, vazamentos, destruições acidentais ou qualquer outra forma de violação. Complementarmente, o princípio da prevenção impõe a adoção de práticas que minimizem os riscos de danos decorrentes do tratamento inadequado. Já o princípio da não discriminação visa impedir o uso para fins discriminatórios ou abusivos. Por fim, a responsabilização e prestação de contas asseguram que os agentes envolvidos demonstrem a adoção de posturas efetivas e conformes aos preceitos legais, respondendo por eventuais prejuízos.

Sequencialmente, imprescindível pormenorizar o manejo dos dados pessoais sensíveis, descritos no Artigo 5º, II, do mesmo dispositivo legal. Para estes, observa-se o Artigo 11, que autoriza o processamento somente após a aquiescência expressa e destacada do titular, ou em hipóteses excepcionais, como cumprimento de obrigações legais; execução de políticas públicas; realização de estudos com anonimização; tutela da saúde por profissionais ou entidades sanitárias, e prevenção à fraude e segurança em sistemas de identificação. Ademais, veda-se o compartilhamento para fins econômicos, salvo em cenários isolados, a exemplo de portabilidade consentida ou prestação de serviços de saúde suplementar.

Em tese, a atual legislação evidencia a preocupação com a salvaguarda da dignidade e dos direitos fundamentais, fixando limites objetivos e promovendo segurança jurídica no manejo de informações sensíveis. A Emenda Constitucional nº 115, de 10 de fevereiro de 2022,

reforça esse compromisso, ao assegurar o direito à proteção de dados pessoais, inclusive no âmbito digital. Contudo, na prática, a opacidade que permeia as operações de coleta e uso, frequentemente, impede a real compreensão dos dados capturados, bem como, dos objetivos a que se destinam. Nas palavras dos autores supracitados:

> É justamente pelo fato de a coleta e a exploração dos dados pessoais por esses sistemas se dar de forma obscura e, muitas vezes abusiva, que se impõe a tutela jurisdicional sobre esses dados. Os indivíduos, que são os verdadeiros titulares de seus dados pessoais, terminam por estar sujeitos à violação de sua privacidade sem ao menos se dar conta disso. Surge então o chamado problema de assimetria informacional, o qual concede maior poder a quem trata os dados pessoais em detrimento aos titulares desses dados. Nesse azo, o cidadão não dispõe de meios de se defender ou conhecer o que de fato é feito com seus dados pessoais, estejam esses na mão das empresas ou do próprio Estado, de modo que, ao passo que aumenta o tratamento dos dados pessoais, diminui a possibilidade de o cidadão saber o que é feito com seus dados. (BARBOSA; SILVA, 2019, p. 494)

Por conseguinte, dada a estreita relação das referidas práticas com direitos fundamentais salvaguardados no ordenamento jurídico, imperativo examinar, com acuidade, o arcabouço normativo aplicável em casos de falhas ou prejuízos oriundos da coleta, manipulação e utilização inadequada de dados pessoais. A análise é ainda mais imprescindível diante da complexidade dos sistemas inteligentes, que, frequentemente, dificultam a identificação dos agentes descritos na legislação, comprometendo a devida responsabilização e a observância plena das garantias legais asseguradas aos titulares.

2.2 O Código de Defesa do Consumidor e a Proteção de Dados

Clarifica-se que o Código de Defesa do Consumidor (Lei nº 8.078/1990) idealiza uma construção normativa vital para a salvaguarda dos direitos consumeristas, fortificando mecanismos jurídicos que atenuam as desigualdades intrínsecas às relações de consumo. Impreterivelmente, este se mantém categórico, especialmente em um contexto marcado pela ascensão das tecnologias digitais, onde dados pessoais são massivamente coletados e explorados – muitas vezes sem o consentimento expresso dos titulares. Nesse sentido, a interação com legislações complementares, tais como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, robustece o arcabouço protetivo, agregando diretrizes específicas, que dizem respeito ao tratamento e à privacidade das informações, inclusive na esfera cibernética.

A priori , a proteção de dados, referenciada enquanto temática central, na Sociedade da Informação, exerce impacto profundo e multidimensional, em âmbitos jurídico e social. Erigido à condição de direito fundamental pelo Artigo 8º da Carta de Direitos Fundamentais da

União Europeia, tal princípio encontra ressonância no ordenamento jurídico brasileiro, particularmente nas disposições do CDC, que objetivam resguardar os consumidores contra os riscos inerentes à coleta e ao tratamento de dados pessoais. A vulnerabilidade destes, solidificada pelo Artigo 4º, I, constitui um dos preceitos das relações consumeristas, tendo em vista o desequilíbrio técnico, econômico e informacional existente entre consumidores e fornecedores. De forma análoga, a LGPD demonstra essa preocupação ao exigir que o tratamento de dados pessoais siga padrões de segurança e boas práticas (Artigo 46), e observe os princípios da necessidade, minimização e responsabilidade (Artigo 6º), reconhecendo, implicitamente, o tratamento de dados como uma atividade de risco.

Adiante, conforme enfatizado pelo Manual de Proteção de Dados Pessoais (2010, p. 9), "a abundância da informação passível de ser obtida sobre o consumidor pode caracterizar uma nova vulnerabilidade deste em relação àqueles que detêm suas informações", destacando, assim, a urgência de instrumentos jurídicos capazes de mitigar as assimetrias informacionais exacerbadas no ambiente digital. Nesse panorama, o Artigo 4º, inciso III, do CDC, assume protagonismo ao promover a harmonização de interesses entre consumidores e fornecedores, equilibrando o desenvolvimento econômico e tecnológico com a proteção dos direitos fundamentais, de modo a consolidar um mercado ético e equitativo. O preceito conecta-se, diretamente, ao princípio da autodeterminação informativa, que consagra um sustentáculo para o tratamento responsável de dados pessoais.

Paralelamente, o direito à segurança, trazido pelo Artigo 6º, inciso I, do CDC, revela-se estratégico ao abarcar, além da proteção relativa à oferta de produtos e serviços, a gestão diligente dos dados pessoais coletados. Em conjunção com o Artigo 43, tal dispositivo consolida diretrizes voltadas à utilização de bancos de dados, visando equilibrar interesses comerciais, defender o consumidor e coibir práticas abusivas. Contudo, reconhece-se que "os dados pessoais do consumidor estão presentes em diversas outras fases da relação de consumo, em várias situações que, dificilmente, podem ser ponderadas utilizando-se, estritamente, as regras do Artigo 43 do Código de Defesa do Consumidor" (BRASIL, 2010, p. 12). Concomitantemente, resta evidenciada a indispensabilidade de legislações complementares, como a LGPD, que agrega camadas adicionais de regulação e segurança ao ambiente cibernético.

Ademais, o direito à informação clara e precisa, previsto nos Artigos 6º, inciso III, e 31, do CDC, destaca um componente implacável na busca pelo equilíbrio das relações consumeristas. Os referidos dispositivos visam assegurar que os consumidores compreendam, integralmente, os produtos, serviços e condições contratuais a que se submetem, aplicando-se,

igualmente, ao meio digital, onde termos de adesão e políticas de privacidade, por exemplo, frequentemente se apresentam de forma obscura e inacessível. Nessa perspectiva, a ausência de transparência no tratamento de dados pessoais é tida como prática abusiva, em flagrante detrimento dos direitos dos consumidores. Veja-se:

> Destacou-se uma crônica falta de transparência no fornecimento de informações claras sobre a utilização e consequências do tratamento dos dados pessoais de seus usuários, bem como a debilidade de muitos sistemas de controle de exposição dos dados pessoais, configurando-se uma situação de clara desvantagem para o consumidor que enseja tanto a aplicação das normas de proteção ao consumidor quanto de normas específicas destinadas à regulação da proteção de dados nas redes sociais. (BRASIL, 2020, p. 112)

Sequencialmente, o Artigo 7º, parágrafo único, do CDC, conjectura a responsabilidade solidária entre os diversos integrantes da cadeia de fornecimento, explicitando inestimável relevância no quadro das relações digitais. As referidas interações, caracterizadas pela colaboração de múltiplos atores — como controladores e operadores de dados —, demandam a aplicação da solidariedade para garantir que o consumidor esteja apto a reivindicar reparação por danos, contra qualquer participante do processo, independentemente de qual tenha sido o efetivo autor do prejuízo. À luz dos ensinamentos de Fernando Antonio Tasso (2020, s.p.), a solidariedade é elemento indeclinável em estruturas complexas, especialmente aquelas que envolvem o uso e o tratamento de informações pessoais, com vistas à proteção do consumidor de entraves na identificação do agente principal responsável.

Outrossim, sobressai, no CDC, o regime de responsabilidade civil objetiva, imposto aos fornecedores de bens e serviços, consoante a inteligência dos Artigos 12 e 14. A sistemática, que também abrange práticas inadequadas no trato de dados pessoais, dispensa a necessidade de demonstrar culpa, exigindo apenas a comprovação do vínculo entre o dano sofrido e a conduta do fornecedor. Ao facilitar o acesso à reparação, a abordagem não apenas fortalece os direitos consumeristas, mas também promove maior eficiência na reparação de danos, sejam eles materiais ou morais, resultantes de falhas relacionadas à privacidade e à segurança no ambiente digital.

> Identifica-se que, no atual panorama Constitucional e infralegal, a relação entre os microssistemas não é de mera intersecção, mas de continência, na medida em que a toda e qualquer violação de direito do consumidor deve-se atribuir, dentre os regimes jurídicos elegíveis, o que melhor atenda à defesa do consumidor. Uma vez tendo se estabelecido que a Lei Geral de Proteção de Dados adotou, como regra, a responsabilidade civil subjetiva, a melhor interpretação parece ser no sentido da derrogação legal em favor da responsabilidade objetiva, nas hipóteses previstas no Código de Defesa do Consumidor. (TASSO, 2020, p. 113)

Nesse ponto, convém pormenorizar que a LGPD aprimora substancialmente o CDC ao celebrar parâmetros claros para o tratamento de dados pessoais, exigindo transparência e a implementação de medidas que assegurem a inviolabilidade e a integridade das informações. O Artigo 45 reforça a interligação normativa ao dispor sobre a aplicação subsidiária do CDC nas relações de consumo, ampliando as garantias jurídicas, e oferecendo maior proteção aos direitos dos titulares: “Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.”

Indubitavelmente, a sinergia entre as legislações robustece, de modo significativo, o conjunto normativo dedicado à proteção dos dados pessoais, assegurando maior segurança jurídica e ampliando as garantias dos titulares. Nesse cenário, o Marco Civil da Internet, que será explorado em sequência, ao definir os princípios fundamentais de privacidade e sigilo no ambiente digital, firma-se como alicerce central na governança da internet, no Brasil, desempenhando um papel essencial na organização do tema relativo aos dados pessoais.

2.3 O Marco Civil da Internet e Garantias de Privacidade

O Marco Civil da Internet (Lei nº 12.965/2014), ao disciplinar o uso da internet e consolidar garantias fundamentais aos usuários, enriquece o ordenamento jurídico brasileiro. Fruto de um amplo e participativo debate social, o diploma normativo supriu lacunas jurídicas, reconhecendo a internet como um direito essencial, e instituindo mecanismos para a proteção da privacidade, da intimidade e da liberdade de expressão. Ao fazê-lo, busca o equilíbrio entre os avanços tecnológicos e a tutela dos direitos individuais.

No âmbito de seus princípios estruturantes, a privacidade figura como alicerce central, consoante o Artigo 3º, que dispõe sobre a salvaguarda da privacidade (inciso II) e a segurança dos dados pessoais (inciso III). Esses dispositivos não apenas respaldam direitos individuais, mas também demandam a implementação de políticas públicas e ferramentas que garantam a proteção dos usuários frente à intensificação da coleta e armazenamento de dados nas infraestruturas digitais. Para Waleska Duque Estrada Vieira (2017, s.p.), "os pilares estabelecidos pelo Marco Civil transcendem a proteção individual, promovendo um equilíbrio necessário entre inovação e direitos fundamentais". Veja-se:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Continuamente, o Artigo 5º reúne definições técnicas primordiais, que sustentam o entendimento amplo dos conceitos trabalhados pelo Marco Civil da Internet. Entre eles, evidencia-se a descrição da "internet" enquanto um sistema global de interconexão, fundamentado em protocolos lógicos, que exerce papel central na estruturação e governança do ambiente digital. Ademais, o dispositivo delibera, no inciso VI, o conceito de "registro de conexão", que engloba dados cruciais para a percepção dos processos de coleta, armazenamento e eventual rastreamento de informações, assegurando maior clareza e confiabilidade jurídica na gestão de dados pessoais.

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Sob esse enfoque, o Artigo 7º intensifica a curatela legal, garantindo a inviolabilidade da intimidade e da vida privada – com previsão de compensação por transgressões –, e restringindo a quebra do sigilo das comunicações à determinação judicial, conforme os limites

legais e o devido processo (incisos I a V). Adicionalmente, exige transparência no tratamento de dados pessoais, mediante a definição de termos claros que regulamentem as práticas de proteção e uso das informações. Essa obrigação inclui a vedação ao compartilhamento de dados com terceiros sem o consentimento expresso do titular, que deve estar vinculado a finalidades justificadas, legais e previamente especificadas em acordos ou políticas de uso. As estipulações, trazidas pelos incisos VI a IX, reforçam o controle e a segurança do usuário, garantindo maior proteção e aderência às normas.

Posteriormente, a neutralidade da rede, princípio essencial consagrado pelo Artigo 9º, amplifica a igualdade de tratamento dos dados trafegados, impedindo discriminações quanto ao conteúdo, origem ou destino. O preceito é vital para preservar a liberdade de expressão e a circulação de informações no ambiente digital, livre de interferências externas. Masso, Abrusio e Florêncio Filho (2014, s.p.) conjecturam que "a neutralidade da rede representa um pilar indispensável para garantir um ecossistema digital justo e livre de censura ou manipulação", promovendo, assim, um ambiente mais equitativo para todos os usuários.

O Artigo 10 apresenta outro ponto relevante, ao especificar que os dados pessoais e os registros de acesso devem ser manejados com estrita observância à privacidade, ratificando que o sigilo somente poderá ser rompido mediante ordem judicial. A medida visa harmonizar a segurança pública com os direitos individuais, impondo, aos provedores, a obrigação de adotar salvaguardas rigorosas para garantir a proteção dos dados armazenados.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
> § 3º O disposto no *caput* não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

A obrigatoriedade de observância à legislação brasileira por empresas que atuam no país, prevista no Artigo 11, também constitui elemento central no Marco Civil da Internet,

abrangendo organizações localizadas fora do território nacional. Apesar disso, a aplicação extraterritorial das normas enfrenta dificuldades relevantes, especialmente diante da resistência de grandes corporações globais em colaborar com as autoridades brasileiras. Sobre o tema, Tomasevicius Filho (2014, p. 164 *apud* Vieira, 2017, p. 209) preconiza que "a tentativa de conferir aplicação extraterritorial ao Marco Civil reflete a necessidade de regular práticas globais, mas enfrenta limitações jurídicas e práticas no âmbito internacional". Tal cenário evidencia desafios significativos à plena eficácia da legislação no contexto globalizado.

No que tange à retenção de dados, os Artigos 13 a 17 avançam ao definir obrigações específicas, como a manutenção de registros pelos provedores de conexão por um ano e, no caso dos provedores de aplicações, a guarda de informações de acesso por seis meses. O acesso a esses dados, condicionado à autorização judicial, assegura maior proteção contra abusos e reforça o controle sobre o tratamento de informações sensíveis. Ademais, a regulamentação busca equilibrar o direito à privacidade com as demandas de segurança e fiscalização, consolidando pilares importantes para a governança digital.

Adicionalmente, o MCI deixa clara a responsabilidade subjetiva dos provedores de conexão e aplicações. Nos Artigos 18 e 19, estabelece-se que os provedores não são responsabilizados por danos decorrentes de conteúdos gerados por terceiros, salvo quando descumprirem ordem judicial específica para remoção do material ofensivo. Assim, a responsabilidade civil do provedor decorre, exclusivamente, do não atendimento à determinação judicial, e não de mera omissão na retirada do conteúdo, preservando, desse modo, a liberdade de expressão e restringindo intervenções a casos de ilícito devidamente analisados pelo Judiciário. Contudo, o Artigo 19 tem gerado controvérsias quanto à sua constitucionalidade, pois exige que a vítima prejudicada aguarde decisão judicial para que medidas sejam tomadas, o que pode agravar a extensão do dano indenizável, especialmente pela falta de celeridade na resolução de litígios (TAPEDINO; TERRA; GUEDES, 2023).

De toda forma, impreterivelmente, o Marco Civil da Internet impulsionou os avanços normativos da Lei Geral de Proteção de Dados. Esta, baseando-se nos princípios do consentimento informado e da transparência, firmou diretrizes rigorosas e abrangentes para o tratamento de informações pessoais, alinhando o Brasil às principais referências internacionais em governança de dados. Desse modo, ao reforçar a salvaguarda das garantias individuais no ambiente digital, as referidas legislações se complementam, criando um sistema jurídico sólido, concebido para harmonizar privacidade, segurança e autonomia, frente aos desafios da proteção informacional.

2.4 A Lei Geral de Proteção de Dados Pessoais e seus Impactos na Coleta de Dados

Inexoravelmente, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) consolida a resposta brasileira às demandas internacionais e nacionais, erigindo uma normativa jurídica voltada ao tratamento de dados pessoais, inclusive nos meios digitais, com o escopo de salvaguardar direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural. Para tanto, frisa-se o delineio dos fundamentos e princípios (elencados, alhures, pelos Artigos 2º e 6º) que atuam enquanto pilares para a interpretação e aplicação das disposições legais, propondo diretrizes destinadas a mitigar os riscos associados à manipulação de dados. Outrossim, clarificam-se os requisitos para o processamento de tais atividades, consoante o Artigo 7º, que complementa os conceitos do Artigo 5º, visando assegurar que as operações sejam conduzidas de forma lícita, e em respeito aos direitos dos titulares. Note-se:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> [...]

Sob essa conjuntura, quaisquer transgressões à norma - cujos desdobramentos guardam similitudes com o Código de Defesa do Consumidor e o Marco Civil da Internet –, quando resultarem em danos, ensejam a obrigação reparatória. Consequentemente, nas hipóteses de manejo inadequado dos dados pessoais, incidirão penalidades como: (I) ações indenizatórias individuais; (II) ações indenizatórias coletivas; (III) sanções administrativas aplicadas por órgãos de proteção ao consumidor; e (IV) sanções administrativas impostas pela

Autoridade Nacional de Proteção de Dados (ANPD). Imperioso reforçar que as reprimendas não se limitam ao âmbito civil, embora este seja o enfoque do presente trabalho.

À vista disso, adentrar-se-á na figura da Autoridade Nacional de Proteção de Dados que, com fulcro no Artigo 52 da LGPD, assume função central na aplicação de penalidades administrativas, incluindo advertências; multas de até 2% do faturamento da empresa (limitadas a R$ 50 milhões por infração); bloqueio de dados; suspensão de atividades e, em casos graves, proibição total de operações relacionadas ao tratamento de dados pessoais. Entretanto, para além do caráter fiscalizatório e sancionatório, a entidade também desempenha papel de natureza normativa e deliberativa, sendo responsável pela interpretação da LGPD, e podendo estabelecer normas e diretrizes para a sua implementação (GETPRIVACY, 2019).

Portanto, os titulares dos dados podem recorrer à ANPD para reivindicar o cumprimento dos direitos homologados pela LGPD, nos termos do Artigo 18, § 1º. A permissividade se estende aos órgãos de defesa do consumidor, que estão aptos a oferecer amparo legal (Artigo 18, § 8º). Depreende-se que a coordenação entre as instituições é reforçada pelo Artigo 52, § 2º, que evidencia que as sanções da LGPD não substituem outras responsabilidades civis, administrativas ou penais, previstas em legislações específicas, como é o caso das entidades de proteção aos consumidores, que também têm poderes sancionatórios no âmbito do Código de Defesa do Consumidor. Dessa forma, na seara das relações consumeristas, o tratamento ilícito de dados pessoais poderá ensejar a aplicação do disposto pelo Artigo 56 do CDC. Veja-se:

> Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:
> I - multa;
> II - apreensão do produto;
> III - inutilização do produto;
> IV - cassação do registro do produto junto ao órgão competente;
> V - proibição de fabricação do produto;
> VI - suspensão de fornecimento de produtos ou serviço;
> VII -suspensão temporária de atividade;
> VIII -revogação de concessão ou permissão de uso
> IX -cassação de licença do estabelecimento ou de atividade;
> X -interdição, total ou parcial, de estabelecimento, de obra ou de atividade;
> XI -intervenção administrativa;
> XII -imposição de contrapropaganda.
> Parágrafo único. As sanções previstas neste artigo serão aplicadas pela autoridade administrativa, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo

Observa-se que as referidas sanções administrativas já eram aplicadas, inclusive, antes da entrada em vigor da Lei Geral de Proteção de Dados. Em 2019, por exemplo, o Facebook foi condenado ao pagamento de multa, no valor aproximado de 6 milhões, pela Secretaria Nacional do Consumidor (Senacon), em razão do compartilhamento indevido de dados, ligado ao escândalo *Cambridge Analytica*. Na mesma direção, em 2014, a operadora Oi foi multada, em três milhões e meio, por monitorar o tráfego de consumidores e comercializar as informações com anunciantes (SANTOS; SILVA; PADRÃO, 2021, s.p.). Complementarmente, na esfera civil, o Artigo 42 da LGPD postula que a obrigação de reparar os danos advindos de violações legais é destinada aos agentes de tratamento de dados. Temos:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Nesse ponto, emerge uma dicotomia substancial ao conjecturar a possível existência de outros responsáveis, que não o controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Artigo 5º, VI) – ou o operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Artigo 5º, VII). Em um cenário marcado pela crescente complexificação dos sistemas inteligentes, é evidente que outros agentes, a exemplo de desenvolvedores, fornecedores e usuários finais, também podem estar envolvidos quando ocorrem irregularidades. Certamente, a opacidade inerente às inteligências artificiais torna desafiadora a identificação dos encarregados pelos métodos de captura e tratamento das informações, sobretudo quando se considera que, conforme discutido alhures, são tratados grandes volumes de dados (*Big Data*), frequentemente obtidos sem o devido consentimento, ou

com transparência insuficiente, o que intensifica os riscos de violações à privacidade e de usos inadequados (DONEDA; WIMMER, 2021, p. 394). Consoante Pedro Domingos (2017):

> Até mesmo os livros sobre big data não explicam o que acontece quando o computador recebe todos esses *terabytes* e magicamente gera novos *insights*. Na melhor das hipóteses, somos deixados com a impressão de que os algoritmos apenas encontram correlações entre pares de eventos, como procurar no Google "remédio para a gripe" e estar gripado. No entanto, encontrar correlações é para o *machine learning* não mais que os tijolos são para as casas, e as pessoas não vivem em tijolos. Quando uma nova tecnologia é tão difusa e revolucionária como o *machine learning*, não é sábio deixá-la como uma caixa preta. A opacidade abre a porta para o erro e a utilização incorreta.

Sequencialmente, elucida-se que a responsabilidade civil, na LGPD, apresenta um escopo de abrangência que demanda análise minuciosa, sobretudo quanto à definição de seu regime jurídico. A priori , destacar-se-á que as violações ocorridas em contextos de relações consumeristas permanecerão sujeitas às disposições do CDC, o qual garante a modalidade objetiva de responsabilização. De outro lado, nos casos em que não há uma relação de consumo entre o titular dos dados e o agente de tratamento, a aplicação da LGPD ocorre de forma subsidiária, assumindo caráter residual (SANTOS; SILVA; PADRÃO, 2021, s.p.).

No que concerne à modalidade prevista na LGPD, o Artigo 42 define duas hipóteses específicas de responsabilidade solidária entre controladores e operadores, no âmbito de danos causados em violação à legislação de proteção de dados. São elas: (I) quando o operador descumpre obrigações legais ou instruções lícitas estabelecidas pelo controlador; e (II) nos casos em que múltiplos controladores estão diretamente envolvidos no tratamento dos dados pessoais. Ademais, o Artigo 43 elenca as excludentes da obrigação reparatória, atreladas à comprovação de que: (I) não realizaram o tratamento questionado; (II) ainda que o tenham realizado, não houve qualquer violação à legislação; ou (III) o dano resultou, exclusivamente, de culpa do titular ou de terceiros. Finalmente, o Artigo 44 delimita as circunstâncias de tratamento irregular, tal como se verifica:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Nota-se que o legislador, ao não especificar o regime de responsabilidade aplicável, suscitou debates teóricos que delineiam duas correntes principais. A primeira defende a responsabilidade objetiva dos agentes de tratamento, dispensando a comprovação de culpa, e vinculando o dever de reparar aos riscos inerentes à atividade desempenhada. A interpretação apoia-se em princípios como segurança, prevenção e responsabilização, que evidenciam o objetivo da LGPD de mitigar riscos intrínsecos ao manuseio de dados. A similitude com o CDC, na proteção de vulneráveis, e dispositivos como o Artigo 43, que apresenta excludentes taxativas, reforçam essa tese, ao sugerirem um regime objetivo, baseado na observância de padrões de legalidade (SANTOS; SILVA; PADRÃO, 2021, s.p.).

Por outro lado, a corrente subjetivista sustenta que a responsabilidade civil, na LGPD, requer a comprovação de culpa, fundamentando-se no histórico legislativo - que afastou referências à responsabilidade objetiva -, e na criação de parâmetros de conduta específicos para os agentes de tratamento. A perspectiva enraíza-se no cumprimento de deveres legais, como segurança e governança, e é reforçada pelo Artigo 6º, inciso X, que destaca a responsabilização e prestação de contas, exigindo a comprovação das diligências por parte dos agentes. Defensores dessa visão argumentam que a adoção da responsabilidade objetiva poderia desestimular avanços tecnológicos, aumentar demandas indenizatórias e gerar insegurança jurídica (SANTOS; SILVA; PADRÃO, 2021). Concomitantemente, frente à ausência de consenso doutrinário, imperioso o exame de caso concreto, sob as perspectivas da LGPD, CDC e MCI, conforme será exposto.

CAPÍTULO 3 – O CASO TIKTOK: COLETA INDEVIDA DE DADOS PESSOAIS E RESPONSABILIDADE CIVIL

A partir da análise conduzida, a Lei Geral de Proteção de Dados firma-se como uma resposta normativa no Brasil, prevendo, face à intensa massificação da coleta e tratamento de dados pessoais, o respeito à autodeterminação informativa (Artigo 2º, II), essencial para a futura discussão do presente trabalho. À luz dos ensinamentos de Danilo Doneda (2014, p. 143), este não se limita à autorização inicial para o manejo de dados, mas implica na participação ativa do titular em todas as fases do processo, incluindo o dever de informação e a transparência. A decisão histórica do Tribunal Constitucional Federal Alemão, de 1983, no caso do censo populacional, é amplamente reconhecida como marco para a consolidação do referido direito. Na sentença, o Tribunal valida que o processamento moderno de dados pessoais, sem limites claros, ameaça, diretamente, a liberdade e a personalidade do indivíduo. Consoante Laura Schertel Ferreira Mendes Pereira (2017, p. 27):

> A designação "direito à autodeterminação informativa" foi utilizada pelo tribunal federal constitucional alemão no âmbito de um processo relativo a informações pessoais coletadas durante o censo de 1983. O BFGH considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelos direitos gerais das pessoas garantidos na constituição alemã. Este direito fundamental garante, a este respeito, a capacidade do indivíduo para determinar, em princípio, a divulgação e o uso de seus dados pessoais. As limitações a esta autodeterminação informacional só são permitidas em caso de interesse público primordial.

Nesse cenário, a Corte enfatizou que o direito fundamental à autodeterminação informativa assegura ao titular o poder de decidir sobre a coleta, o uso e a divulgação de seus dados, permitindo limitações apenas em situações de interesse público primordial. A decisão introduziu o conceito de *informationelle selbstbestimmung*, que se tornou referência internacional em matéria de proteção de dados (DONEDA, 2011, p. 95). Contudo, além da base na Constituição alemã, o preceito encontra ressonância no Artigo 22 da Declaração Universal dos Direitos Humanos de 1948, que assegura o livre desenvolvimento da personalidade, e no Pacto Internacional dos Direitos Econômicos, Sociais e Culturais, que reforça a garantia à educação e à participação na esfera pública (GARCIA, 2020, p. 165).

Adicionalmente, Bruno Ricardo Bioni (2019, p. 101-102) endossa que a autodeterminação informativa se mostra indispensável na salvaguarda das liberdades individuais, sobretudo em um contexto de intensos avanços tecnológicos. O consentimento, segundo o autor, desempenha um papel crucial na concretização do direito, permitindo ao titular

manifestar sua vontade, de maneira inequívoca e consciente, conforme estabelece o Artigo 7º da LGPD, que exige clareza e destaque na autorização. Sob essa perspectiva, a autodeterminação informacional ultrapassa a esfera individual, firmando-se como um princípio democrático, que promove a simetria informacional e fortalece direitos fundamentais. Doneda (2014, p. 143) acrescenta que:

> [...] a disseminação do modelo das autoridades independentes para a tutela dos dados pessoais – tanto mais necessárias com a diminuição do poder de 'barganha' com o indivíduo para a autorização ao processamento de seus dados, e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas europeias em matéria de proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas).

Portanto, depreende-se que é garantido, ao indivíduo, o controle sobre o uso de seus dados pessoais, facultando-lhe decidir quem poderá acessá-los, para quem serão compartilhados e para quais finalidades serão utilizados. O direito é profundamente conectado à proteção da privacidade e ao livre desenvolvimento da personalidade, demandando do Estado a criação e execução de políticas públicas eficazes que assegurem a autonomia do titular e a segurança no tratamento de suas informações (SOUSA; SILVA, 2020, p. 11). Outrossim, o consentimento, como eixo central da autodeterminação informativa, deve ser claro, explícito e aplicado em todas as etapas do processamento dos dados. De fato, o instrumento não apenas legitima o uso das informações pessoais, mas também reforça a efetividade prática desse direito, prevenindo abusos e promovendo a transparência no tratamento de dados.

3.1. Inteligência Artificial e o Tratamento de Dados Pessoais

Tendo sido feita a distinção do conceito de autodeterminação informacional, convém analisar sua aplicação no contexto das inteligências artificiais. Inequivocamente, os debates atuais, na internet, têm como foco principal a preocupação com a confiabilidade das informações acessadas pelos usuários. Isso decorre do fato de que a coleta de dados possibilita sua manipulação por meio do controle dos fluxos informacionais, comumente em detrimento da neutralidade da rede. O cenário é intensificado pelo uso de algoritmos, isto é, ferramentas eletrônicas que processam e filtram os dados disponíveis, permitindo que conteúdos específicos sejam direcionados para cada usuário (GARCIA, 2020, p. 168).

Nesse ponto, urge inferir que os dados pessoais são considerados os insumos principais da economia digital, de modo que, os algoritmos atuam como instrumentos de processamento, transformando informações em resultados utilizados para inúmeras finalidades, como *marketing* personalizado, decisões automatizadas e perfilização de indivíduos. Ao mesmo tempo em que proporcionam inovações significativas, suscitam questões sobre privacidade e os limites éticos e legais aplicáveis, vez que, decisões baseadas em algoritmos impactam, diretamente, na efetivação de direitos. Note-se:

> Como se vê, algoritmos vêm sendo utilizados para análises complexas, que abarcam as respostas para nossas perguntas mais difíceis, como decisões e diagnósticos que, além de representarem uma verdadeira devassa na intimidade das pessoas, ainda terão impactos nas possibilidades e no acesso destas a uma série de direitos e oportunidades. Não é novidade que algoritmos hoje podem decidir quem terá crédito e a que taxa de juros, quem será contratado para trabalhar em determinada empresa, qual a probabilidade de reincidência de determinado criminoso, quem deve ser atropelado em determinadas situações, entre inúmeras outras circunstâncias. O mais preocupante é que tudo isso é feito a partir de uma série de dados que podem até parecer irrelevantes para o cidadão comum, tais como suas buscas na internet, tempo gasto em redes sociais, "curtidas" sobre determinadas questões, músicas e locais de sua preferência, entre outros. É com base nesses dados, que depois são convertidos em novos dados, que a inteligência artificial age para nos trazer um componente crítico da própria inteligência: a predição, considerada um input central para os processos decisórios (FRAZÃO, 2019, p. 32-33).

Sob essa conjuntura, a crescente popularização dos modelos computacionais, no tratamento de dados, impulsiona o "capitalismo de vigilância", marcado pela exploração do excedente comportamental (*behavioral surplus*). A prática amplifica a vigilância sobre os indivíduos, ao coletar dados além do necessário para aprimorar serviços e desenvolver projeções cada vez mais precisas sobre comportamentos e preferências (ZUBOFF, *apud* FRAZÃO, 2019, p. 33). Desse modo, as inferências algorítmicas, frequentemente desprovidas de supervisão humana, abrem margem para erros e distorções. Yuval Noah Harari (2018, p. 15) adverte: "algoritmos de *Big Data* poderiam criar ditaduras digitais, nas quais todo o poder se concentra nas mãos de uma minúscula elite, enquanto a maior parte das pessoas sofre não em virtude de exploração, mas de algo muito pior: irrelevância."

Consequentemente, a expansão descontrolada de tais sistemas não só compromete a privacidade, como também ameaça princípios fundamentais consolidados pelo Código de Defesa do Consumidor, Marco Civil da Internet e Lei Geral de Proteção de Dados, com destaque para a autodeterminação informacional. Julie Cohen (2000) enfatiza que a lógica algorítmica privilegia padrões estáticos e objetivos, negligenciando formas mais dinâmicas de conhecimento humano, o que enfraquece a liberdade individual, ao moldar comportamentos

com base em trajetórias predefinidas. Nesse panorama, as tecnologias categorizam os indivíduos e influenciam, diretamente, suas decisões e opiniões, caracterizando o que Stefano Rodotà (2008) descreveu como uma "sociedade da classificação", na qual a manipulação, amplamente explorada em campanhas de *marketing* e políticas, por exemplo, aprofunda desigualdades sociais e fragiliza os pilares democráticos. Veja-se:

> Não obstante a ausência de transparência e *accountability*, os sistemas de inteligência artificial que movem a economia digital são programados para produzirem inferências e predições, com as quais se pode classificar as pessoas e, a partir daí, determinar os seus destinos, inclusive no que diz respeito ao seu acesso a direitos e oportunidades. Ocorre que tais processos, ainda mais se forem totalmente automatizados e sem nenhum tipo de controle humano, podem ser fontes inesgotáveis de julgamentos equivocados e que reproduzam e intensifiquem ainda mais desigualdades e discriminações. Por essas razões, todas as modificações apontadas, longe de se restringirem apenas à economia, apresentam importantes consequências também para a política, à sociedade e às próprias dimensões existenciais dos cidadãos, que passam a sofrer permanente ataque em diversas perspectivas, inclusive naquelas que dizem respeito à própria individualidade, cada vez mais comprometida diante do crescente poder de manipulação que decorre do processamento de dados. Fica claro, assim, que não é exagerada a citação de Yuval Harari [...] (FRAZÃO, 2019, p. 49).

No Brasil, a LGPD, embora não seja especificamente direcionada aos processos algorítmicos, visa estabelecer-se como um referencial jurídico apto a enfrentar a falta de transparência e a ausência de responsabilidade que permeiam tais sistemas, frequentemente designados como "caixas-pretas". A opacidade inerente aos mecanismos de inteligência artificial contribui para a perpetuação de práticas abusivas, reforça desigualdades estruturais e compromete, de forma expressiva, a autodeterminação informacional dos titulares de dados. Conforme destaca Frank Pasquale *apud* Ana Frazão (2019, p. 41), a obscuridade deliberadamente mantida por grandes corporações e governos não apenas atenta contra direitos fundamentais, mas também compromete o equilíbrio do desenvolvimento econômico sustentável, ameaçando a integridade das bases que sustentam as democracias contemporâneas.

Não obstante, Pasquale (Ibid., p. 42) explicita que a opacidade e a falta de transparência, nos mercados digitais, não são consequências naturais, mas resultam de ações deliberadas, por parte de grandes agentes econômicos e estatais. Esses atores empregam estratégias variadas, desde proteções jurídicas, como o sigilo comercial, até práticas não regulamentadas, criando um ambiente de obscuridade que lhes permite monitorar, classificar e avaliar indivíduos, enquanto mantêm suas metodologias em segredo, “inclusive para o fim de proteger sua valorosa propriedade intelectual”. Mediante, a abordagem ultrapassa questões técnicas, de modo que, compromete a liberdade inerente à internet, restringe o acesso à informação e coage direitos individuais.

Para enfrentar os desafios éticos e técnicos associados à inteligência artificial, a professora Virgínia Dignum propõe o método ART, composto pelos princípios de *accountability, responsibility* e *transparency*. O primeiro deles exige que as máquinas sejam capazes de justificar suas decisões, oferecendo explicações claras que permitam rastrear e compreender os processos internos. Entretanto, a exigência encontra obstáculos significativos nos sistemas de aprendizado de máquina, especialmente aqueles com arquiteturas complexas, nos quais os mecanismos de ponderação e escolha, muitas vezes, permanecem inacessíveis ou incompreensíveis, devido à própria estrutura do modelo algorítmico.

O princípio da *responsibility* foca na relação entre humanos e IA´s, enfatizando a necessidade de atribuir responsabilidade às partes envolvidas na interação homem-máquina. Isso inclui operadores, desenvolvedores e instituições que se beneficiam das decisões algorítmicas. Casos emblemáticos, envolvendo a coleta indevida de dados ou ferramentas de vigilância que violam a privacidade de terceiros, ilustram como a ausência de delimitação clara sobre responsabilidades pode gerar abuso. A lacuna viabiliza que indivíduos ou organizações desfrutem das ações da máquina - mesmo quando estas não foram diretamente programadas -, ampliando a importância de estabelecer critérios de responsabilização (DIGNUM, 2019).

Por fim, o princípio da *transparency* visa garantir que os processos de decisão das IA´s sejam compreensíveis e auditáveis, incluindo o entendimento do funcionamento interno da máquina e a procedência dos dados utilizados. Contudo, a transparência encontra óbices no contexto corporativo, vez que, o sigilo comercial é frequentemente invocado para justificar a não divulgação de códigos e metodologias. A falta de visibilidade dificulta a avaliação ética e técnica das IA´s, limitando a possibilidade de assegurar o respeito aos direitos fundamentais e valores sociais (DIGNUM, 2019). Portanto, Dignum assevera que superar as referidas barreiras é essencial para a promoção de uma governança responsável da inteligência artificial.

Assim, elucidar-se-á como os conceitos repercutem em um caso concreto, a exemplo do TikTok. A plataforma, amplamente reconhecida pelo emprego sofisticado de inteligência artificial na curadoria personalizada de conteúdos, modela um cenário promissor para reflexões éticas e jurídicas. Desde 2020, o TikTok tem se destacado pela massiva coleta de dados pessoais, incluindo preferências de consumo, padrões de interação e localização geográfica. Tal prática suscita inquietações acerca da opacidade dos algoritmos empregados e dos possíveis efeitos de manipulação comportamental sobre os usuários.

3.2. Coleta Indevida de Dados Pessoais: o caso TikTok no Brasil

Constata-se que, em 2020, o Instituto Brasileiro de Estudo e Defesa das Relações de Consumo (IBEDC/MA) ajuizou Ação Coletiva de Consumo (0816292-73.2020.8.10.0001 – TJMA) em face da empresa BYTEDANCE BRASIL TECNOLOGIA LTDA. (TikTok), alegando práticas abusivas e violação de direitos fundamentais. O litígio, alicerçado na salvaguarda da privacidade e das informações pessoais, expôs a coleta biométrica indevida, ausência de transparência no funcionamento das operações, e exploração econômica de dados pessoais sensíveis dos consumidores. Ressalte-se que a referida demanda, no Brasil, refletiu a repercussão das numerosas denúncias relacionadas aos vícios de segurança e tratamento de dados dos usuários, pelo TikTok, que resultaram em investigações e processos judiciais, precipuamente nos Estados Unidos (IBEDEC/MA, 2020).

A priori , afirma-se que, no caso em voga, a relação de consumo está plenamente caracterizada, consoante o Artigo 5º, inciso XXXII, da Constituição Federal, que assegura a defesa do consumidor, e o CDC, que define o consumidor como o destinatário final (Artigo 2º) e o fornecedor como aquele que realiza atividades de comercialização ou prestação de serviços (Artigo 3º). A empresa, ao ofertar serviços digitais, enquadra-se no conceito de fornecedora, tornando o CDC plenamente aplicável, ainda que a remuneração se dê de forma indireta, em obediência à jurisprudência consolidada pelo STJ.

À posteriori, infere-se que a demandada, operadora da plataforma TikTok — aplicativo de compartilhamento de vídeos, que permite a criação e divulgação de conteúdos sobre variados temas —, disponibiliza múltiplas funcionalidades, entre as quais se destacam os filtros faciais. Por meio desses, há a sobreposição de elementos ao rosto, que modificam características faciais dos usuários e exigem, para tanto, a captura e o mapeamento de dados biométricos. Isto é, “geometria biologicamente ínsita aos pontos dos desenhos faciais” (IBEDEC/MA, 2020), que digitaliza informações únicas e sensíveis. Embora apresentados como ferramentas lúdicas, até o ajuizamento da ação, os filtros operavam sem consentimento expresso e esclarecido, configurando prática abusiva e indiscriminada, que vulnerabilizou os titulares, mascarando-se pelo aparente caráter inofensivo. Inequivocamente, houve violação à privacidade biométrica, e desrespeito aos princípios basilares da transparência e autodeterminação informativa.

Ademais, à época, as políticas de privacidade e os termos de uso mostravam-se vagos e insuficientes, omitindo informações essenciais acerca da finalidade específica da coleta, do período de retenção dos dados e dos terceiros que poderiam acessá-los. Não havia objetividade quanto à extensão das atividades relacionadas à captura, recebimento, armazenamento, compartilhamento e utilização dos dados biométricos. Embora a plataforma alegasse

comprometimento com a segurança, na prática, desviava-se do dever de clareza em relação ao tratamento conferido às informações captadas, deixando de apresentar garantias concretas quanto à proteção de dados sensíveis. Oportuno frisar as palavras da própria:

> A segurança dos seus dados pessoais:
> Tomamos medidas para garantir que as suas informações são tratadas de forma segura e de acordo com esta política. Infelizmente, a divulgação de informação na Internet não é totalmente segura. Embora envidemos todos os esforços para proteger os seus dados pessoais, não podemos garantir a segurança das informações divulgadas através da Plataforma; quaisquer divulgações são por sua própria conta e risco.

Nesse contexto, conforme destacado pelo IBEDEC/MA (2020), a ré, nocivamente, "implementou, no aplicativo, uma ferramenta de inteligência artificial que automaticamente digitaliza o rosto de indivíduos, de modo, então, a coletar, capturar, receber, obter, armazenar e usar digitalizações faciais sem obtenção do consentimento de usuários". A gravidade é exacerbada em razão do caráter singular e intransferível conferido à biometria facial, amplamente adotada para acesso a conteúdos confidenciais, a exemplo de contas bancárias. Portanto, a violação dos dados, classificados como sensíveis (Artigo 5º, II, da LGPD), submete os indivíduos a riscos substanciais, incluindo fraudes financeiras, roubo de dados e invasões de intimidade. Sob essa ótica, a *Federal Trade Commission* (FTC), agência americana de proteção ao consumidor, já apontou que dados biométricos possuem alta relevância no mercado de dados, sendo amplamente manipulados por grandes corporações. No presente caso, a demandada, além de utilizar as informações para fins comerciais, comprometeu o princípio da anonimização, elaborando perfis detalhados dos usuários e explorando-os economicamente, por meio de publicidade direcionada. Veja-se:

> Em síntese, a Ré passa a explorar economicamente as informações colhidas dos usuários, acumulando perfis mais detalhados, aumentando seus negócios de publicidade, comercializando sua capacidade de segmentar anúncios com base em seus perfis pessoais pormenorizados, direcionando mais anúncios para seus serviços pagos e, assim, gerar receita. É importante salientar que tais dados, de chofre, também alcançam alta valia no mercado paralelo de transmissão ilegal de dados (IBEDEC/MA, 2020).

Concomitantemente, a requerida negligenciou o cumprimento de suas obrigações no âmbito negocial, transgredindo não apenas os deveres de transparência e respeito às normas legais de proteção à privacidade, mas também "os princípios fundamentais de harmonização, lealdade e equilíbrio nas relações de consumo" (IBEDEC/MA, 2020). Ao adotar práticas voltadas à maximização de lucros, estruturou um modelo tecnológico que ocultava, dos

consumidores, os riscos atrelados ao uso do aplicativo, especialmente no que tange à segurança dos dados pessoais. Como resultado, os usuários foram colocados em uma posição de significativa vulnerabilidade, sem acesso a informações claras ou mecanismos de proteção efetivos.

Outrossim, apurou-se que o aplicativo recolhia dados em volume muito superior ao necessário para seu funcionamento, gerando preocupações quanto à possibilidade de: I) transferência de informações para jurisdições desprovidas de regulamentação adequada; II) compartilhamento ou comercialização de dados com terceiros sem critérios claros; e III) armazenamento indefinido das informações, mesmo após a exclusão da conta pelo usuário. Esses fatores acentuaram as inquietações relacionadas à salvaguarda dos dados, especialmente frente à ameaça de vazamentos ou acessos não autorizados aos bancos de dados da plataforma, bem como, àqueles mantidos por terceiros. A suspeita de que essas informações eram compartilhadas com a anuência implícita da empresa apenas reforçou a seriedade da situação, asseverando um quadro de desrespeito às práticas de proteção à privacidade e à segurança dos usuários (IBEDEC/MA, 2020). Note-se:

> No caso vertente, ao fim e ao cabo, a Requerida não exerceu o mister correto em todo o trilho negocial, derruindo-se no que toca à transparência do aplicativo, desrespeitando em diversos sentidos as normas legais de proteção à privacidade, olvidando-se, pois, de limites prudentes e necessários à fluidez da relação jurídica, vulnerando, em amplitude, também, a segurança seus usuários como um todo, expondo-os a maiores riscos, tais como fraudes, roubos de dados, invasão da intimidade. Fica robusto, pois, que a conduta coloca os consumidores em situação de extrema desvantagem, mormente porque a empresa planejou e articulou esse desenho tecnológico para gerar receita, de modo que impossibilita que o consumidor saiba que o aplicativo é nocivo quanto à segurança de seus dados. A problemática se agrava com a possibilidade de que esses dados sensíveis sejam compartilhados em mercados paralelos de transmissão ilegal, onde possuem elevado valor econômico. Ademais, a coleta massiva e sem controle permite desvendar o comportamento individual dos usuários, suas relações sociais e preferências privadas, expondo-os a invasões de privacidade e a uma vigilância generalizada. O Conselho de Direitos Humanos das Nações Unidas já repudiou práticas similares, reconhecendo os riscos de tais condutas para a segurança e a autonomia dos indivíduos (IBEDEC, 2020).

Urge inferir, nesse ponto, que os dados pessoais sensíveis demandam atenção especial, face à gravidade e amplitude dos prejuízos decorrentes do seu manejo inadequado, os quais apresentam alto risco de emergir discriminações e desigualdades. Caitlin Mulholland (2021, p. 8-9) defende que o amparo legal deve ser concebido como uma extensão do direito à privacidade ou, em certos casos, do direito à identidade, tendo a autodeterminação informativa como eixo central. A autora delineia sua vinculação ao direito fundamental à igualdade, previsto no Artigo 5º, *caput*, da Constituição Federal, que veda qualquer forma de distinção ou

discriminação. Além disso, ressalta o Artigo 3º, que estabelece, como objetivo, a promoção do bem-estar geral, livre de preconceitos e segregações. Tais preceitos reforçam a necessidade de um tratamento de dados pautado na equidade e no respeito à dignidade humana.

Por conseguinte, as condutas adotadas pelo TikTok ultrapassaram os limites prudenciais impostos pelo ordenamento jurídico, acarretando severas violações, especificamente, aos Artigos 1º, III, e 5º, X e XII, da Constituição Federal, além de desrespeitarem compromissos internacionais, como o Pacto Internacional de Direitos Civis e Políticos e o Pacto de San José da Costa Rica. Diante das transgressões evidenciadas, tornou-se indispensável a responsabilização judicial da requerida, visando a salvaguarda dos direitos fundamentais dos consumidores e o restabelecimento da equidade nas relações consumeristas.

3.3. Aplicação da Responsabilidade Civil à Coleta de Dados pelo TikTok

Inexoravelmente, o julgamento da Ação Coletiva demarcou precedente jurídico de incidência da responsabilidade civil ao contexto da coleta indevida de dados pessoais, por sistemas inteligentes. Considerando o atual cenário de lacunas legislativas específicas para regulamentar, integralmente, as práticas voltadas às tecnologias das IA´s, o caso foi analisado à luz do ordenamento vigente, ratificando parâmetros essenciais de proteção de dados e direitos consolidados pelos usuários. A decisão, emanada da Vara de Interesses Difusos e Coletivos de São Luís, explorou, de forma contundente, os deveres de transparência, boa-fé e equilíbrio nas relações consumeristas, reafirmando a imprescindibilidade de harmonizar o avanço tecnológico com a tutela da privacidade e da dignidade, em esfera digital.

No âmago da controvérsia, conjecturou-se a utilização de tecnologias alicerçadas em inteligência artificial, para fins de captura, armazenamento e compartilhamento de dados biométricos, sem o consentimento livre, expresso e informado. A prática evidenciou violação direta à autodeterminação informativa, assegurada pelo Artigo 5º, inciso LXXIX, da Constituição Federal, introduzida pela Emenda Constitucional nº 115/2022, e reforçada por legislações infraconstitucionais, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Outrossim, a coleta indiscriminada de dados sensíveis afrontou direitos constitucionais à privacidade, intimidade e honra, previstos no Artigo 5º, incisos X e XII, e desrespeitou o Artigo 21 do Código Civil, que salvaguarda a vida privada. Também foram desconsiderados inúmeros dispositivos do Código de Defesa do Consumidor, incluindo os Artigos 4º, III; 6º, III; 20, §2º; 39 e 51, IV, que exigem transparência, boa-fé e equilíbrio nas relações de consumo.

Em sequência, a sentença apontou patentes transgressões à Lei Geral de Proteção de Dados, especialmente aos Artigos 5º, inciso II, que caracteriza os dados sensíveis; 6º, que consagra os princípios da finalidade, necessidade e proporcionalidade; 7º, inciso I, que condiciona o tratamento dos dados ao consentimento livre, específico e inequívoco; e 11, que impõe restrições rigorosas à manipulação de informações biométricas. Simultaneamente, constatou-se o descumprimento do Artigo 7º, incisos VIII e IX, do Marco Civil da Internet, que estabelece a obrigatoriedade de informações claras e de assentimento categórico, para a captura e manuseio de dados pessoais. Nesse caminhar, a análise dos autos revelou que os termos de uso e as políticas de privacidade da plataforma apresentavam linguagem excessivamente vaga, o que impossibilitava, aos consumidores, a compreensão plena acerca da abrangência do uso de seus dados, os terceiros que poderiam acessá-los e o período de retenção das informações, celebrando evidente contrariedade aos direitos fundamentais de privacidade e à transparência nas relações consumeristas. Veja-se:

> A mencionada lei ainda determina que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (art. 11). Esses dispositivos do Marco Civil da Internet, ao estabelecerem a proteção da privacidade e dos dados pessoais, estão em consonância com o direito à autodeterminação informativa, que encontra suas bases no direito constitucional à privacidade e à proteção de dados. Dada sua densidade normativa, em 2018, foi positivado na Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que, ao reconhecer a importância da autodeterminação informativa, reforça a proteção dos dados pessoais como um elemento essencial para a preservação da privacidade e da liberdade individual. A autodeterminação informativa compreende a capacidade do indivíduo de controlar suas próprias informações, decidindo sobre sua coleta, utilização e compartilhamento por terceiros. Dessa forma, o arcabouço jurídico brasileiro solidifica a proteção do direito fundamental à privacidade e à proteção de dados no ambiente da internet. Assim, a coleta, uso e o tratamento indevido de dados de usuários, sem o necessário livre consentimento, configura violação dessas normas. Na hipótese dos autos, verifico que o réu, em sua defesa, argumentou ausência de violações à boa-fé, informação, lealdade e transparência, afirmando que não há na plataforma do aplicativo TikTok qualquer dispositivo que proceda com a coleta dos dados dos usuários a partir da biometria facial. Aduziu, ainda, que a plataforma não permite o compartilhamento de dados com terceiros, conforme alega o instituto autor. As evidências constantes dos autos, entretanto, indicam o contrário (TJMA, 2024).

Sob tal conjuntura, as evidências probatórias ainda revelaram que a requerida já havia firmado acordos judiciais, nos Estados Unidos, em razão de práticas análogas, relacionadas à coleta irregular de dados sensíveis e executadas por sistemas de IA. Entretanto, a origem precisa da irregularidade permaneceu envolta em incerteza, haja vista não ter sido possível determinar se a conduta era fruto de programação deliberada, ou decorria da autonomia do aprendizado de

máquina (*machine learning*). A indefinição acerca do funcionamento dos sistemas inteligentes inviabilizou a individualização da falha, levando à imputação de responsabilidade objetiva à empresa, na condição de fornecedora do serviço. A relação entre os consumidores e a plataforma foi juridicamente enquadrada como de consumo, ainda que os serviços fossem disponibilizados sem cobrança direta. Isso porque, segundo entendimento consolidado pelo Superior Tribunal de Justiça, o conceito de remuneração abrange também os ganhos indiretos, como a exploração econômica dos dados pessoais coletados. Portanto, a responsabilidade objetiva do TikTok foi fundamentada no Artigo 14 do CDC, que impõe, aos fornecedores, o dever de reparar prejuízos oriundos de falhas na prestação de serviços, independentemente de culpa *lato sensu*.

Ao analisar os elementos tradicionalmente estruturantes da responsabilidade civil, compreendidos pela conduta humana, dano e nexo causal, observa-se que, de certo modo, todos foram delineados no contexto em voga. Embora a conduta – revestida de ato ilícito - não tenha sido diretamente individualizada, foi presumida, em razão da posição da empresa enquanto fornecedora do serviço e responsável pela operacionalização da plataforma. O ato ilícito, por sua vez, manifestou-se na coleta de informações biométricas, sem o consentimento adequado, em evidente transgressão à autodeterminação informativa e aos princípios da necessidade, adequação e proporcionalidade, que regem o tratamento de dados pessoais, conforme preceitua a legislação vigente.

No que tange ao nexo causal, esse foi formalizado entre as práticas negligentes da empresa e os danos ocasionados aos consumidores. Indubitavelmente, em um cenário onde sistemas de inteligência artificial operam com autonomia, surge a necessidade de delimitar responsabilidades. Assim, o ordenamento jurídico, ao se basear na responsabilidade objetiva, prevista no Artigo 14 do Código de Defesa do Consumidor, dispensa a comprovação de culpa, exigindo, apenas, a demonstração do defeito no serviço e do prejuízo sofrido pelos usuários, de modo que, a vinculação entre a falha e os danos experimentados, pela coletividade, corroborou a responsabilização da empresa demandada.

Infere-se que a inexistência de personalidade jurídica atribuída aos sistemas de inteligência artificial, no Brasil, direciona a análise para os agentes tradicionalmente responsáveis na relação jurídica, como desenvolvedores, fornecedores e operadores. Apesar dos avanços, no debate internacional, acerca da "personalidade robótica", exemplificados pelo caso da robô Sophia — dotada de um sofisticado sistema de IA, desenvolvido pela *Hanson Robotics*, e reconhecida, oficialmente, como cidadã da Arábia Saudita, em 2017, com direitos que, paradoxalmente, nem as mulheres daquele país possuem (GALILEU, 2017) —, tal concepção

permanece teórica no contexto jurídico brasileiro. Esse concentra esforços na regulamentação do uso e desenvolvimento da IA, visando conciliar a promoção de avanços tecnológicos com a salvaguarda efetiva dos direitos fundamentais.

No tocante aos danos decorrentes, a decisão foi categórica ao reconhecer tanto o dano moral individual quanto o coletivo. O dano moral individual foi presumido (*in re ipsa*), visto que, a coleta não autorizada de dados sensíveis, como a biometria facial, gera, automaticamente, um abalo à dignidade e à privacidade dos usuários, nos termos dos Artigos 12 e 14 do CDC, bem como, do Artigo 42 da LGPD. Por outro lado, o dano moral coletivo foi caracterizado como um óbice intolerável aos valores fundamentais da coletividade, denotando lesão grave e injustificável, em consonância com o Artigo 6º da Lei nº 7.347/1985, que regula as ações civis públicas, e com precedentes do STJ, que ressaltam a função pedagógica e sancionatória da referida modalidade de indenização. Tem-se:

> Logo, para a demonstração desse tipo de dano, é suficiente a constatação da prática de conduta ilícita que viole direitos de conteúdo extrapatrimonial da coletividade, dispensando-se a necessidade de comprovação de prejuízos concretos. No caso em análise, ocorreu a coleta de dados biométricos de usuários, à revelia da autorização de seus titulares, o que evidencia uma lesão à confiança nas relações negociais, o que gera transtornos significativos à coletividade. O fato representa uma violação séria da privacidade e segurança dos usuários. As consequências desse tipo de violação podem ser amplas e duradouras, afetando a confiança no uso de tecnologias e exigindo medidas rigorosas de proteção de dados por parte das autoridades públicas. Portanto a reparação pelos danos morais coletivos deve ser fixada de modo a desencorajar a reincidência da falta, sem, contudo, propiciar enriquecimento indevido, devendo ser avaliada à luz da proporcionalidade da ofensa (STJ - REsp: 1124471 RJ 2009/0082448-1, Relator: Ministro LUIZ FUX, Data de Julgamento: 17/06/2010, T1 - PRIMEIRA TURMA, Data de Publicação: DJe 01/07/2010; STJ, AgRg no Ag 1.410.038) (TJMA/2024).

Adiante, observa-se que, à luz da jurisprudência pacificada pelo STJ, determinadas condutas, a exemplo da coleta indevida de dados biométricos pelos sistemas de inteligência artificial do TikTok, podem ultrapassar os limites da esfera individual, atingindo a coletividade e configurando o dano moral coletivo. Essa forma de reparação extrapatrimonial, reconhecida como categoria autônoma, não se limita à soma dos danos individuais, mas resulta de uma violação de caráter transindividual, capaz de comprometer a integridade moral da sociedade como um todo. No precedente do REsp 1.057.274, sob relatoria da ministra Eliana Calmon, o STJ firmou que, em situações de violação de interesses difusos ou coletivos, não se exige a comprovação de sofrimento ou abalo psicológico individual, bastando a demonstração de lesão ao coletivo. No presente contexto, a captura não autorizada de dados sensíveis de milhões de usuários caracteriza substancial lesão à confiança coletiva e à privacidade, justificando, assim,

a condenação por dano moral coletivo, fundamentada na necessidade de salvaguarda dos direitos transindividuais.

Não obstante, a condenação da BYTEDANCE BRASIL incluiu o pagamento de 23 milhões de reais, a título de danos morais coletivos, a serem destinados ao Fundo Estadual de Proteção e Defesa do Consumidor (FPDC). Ato contínuo, a empresa foi sentenciada a adimplir R$ 500,00 (quinhentos reais), por danos morais individuais, a cada usuário que comprove a utilização do aplicativo até a atualização de sua política de privacidade, em 2021. Foram impostas, ainda, medidas corretivas, como a abstenção de coletar dados biométricos sem consentimento, a implementação de mecanismos que assegurem maior transparência e clareza no consentimento dos usuários, e a exclusão imediata dos dados obtidos de forma irregular.

A decisão ressaltou a imprescindibilidade de harmonizar o progresso tecnológico com a tutela dos direitos fundamentais, enfatizando a relevância de alinhar a legislação nacional às normativas internacionais de proteção de dados, a exemplo do Regulamento Geral de Proteção de Dados da União Europeia. O julgamento não apenas garantiu a defesa dos consumidores, mas também consolidou um precedente crucial para a regulamentação do uso ético, responsável e transparente de tecnologias alicerçadas em inteligência artificial. Ademais, a atualização da política de privacidade da plataforma, em 2021, ao explicitar a possibilidade de coleta de dados faciais e de voz, corroborou as alegações apresentadas, evidenciando a prática reiterada de transgressões aos direitos dos usuários.

Em continuidade às constatações, em 4 de novembro de 2024, a Autoridade Nacional de Proteção de Dados instaurou processo administrativo sancionador contra o TikTok, exigindo a regularização do tratamento de dados pessoais de crianças e adolescentes. A decisão teve origem em fiscalização iniciada em 2021, que identificou indícios de violações à LGPD, incluindo o descumprimento do princípio do melhor interesse desse público vulnerável, que assegura a prevalência de seus direitos. A ANPD determinou medidas imediatas, como a desativação do recurso "feed sem cadastro", no Brasil, em até 10 dias úteis, e a apresentação, em 20 dias úteis, de um plano de conformidade, para fortalecer os mecanismos de verificação de idade e aprimorar os protocolos de exclusão de contas de crianças. O processo investigará práticas como a coleta irregular de dados sem fundamento legal, e a personalização de conteúdo para usuários do "feed sem cadastro", visando garantir a conformidade legal. Ao final, poderão ser aplicadas sanções, conforme os critérios previstos no regulamento de dosimetria, caso confirmadas novas irregularidades no tratamento de dados pessoais (ANPD, 2024).

CONSIDERAÇÕES FINAIS

Ao alcançar o epílogo desta investigação, emerge um panorama complexo e multifacetado, que reflete a profunda interação entre os desafios técnicos e jurídicos trazidos pelas inteligências artificiais, no contexto da coleta indevida de dados pessoais. A análise empreendida percorreu os pilares da responsabilidade civil, os contornos normativos aplicáveis à proteção de dados e as nuances de um caso emblemático, o TikTok, evidenciando que, embora as normas vigentes sejam eficazes em alguns aspectos, também revelam profundas lacunas na compreensão e regulação das peculiaridades tecnológicas.

Sob um prisma histórico-evolutivo, percebe-se que a responsabilidade civil, ancorada em elementos como conduta humana, dano e nexo causal, mostra-se insuficiente para abarcar a singularidade das inteligências artificiais. Tais sistemas, regidos por algoritmos opacos e decisões autônomas, desarticulam a linearidade tradicional entre ação e consequência. A dificuldade em identificar a conduta humana direta que configure ato ilícito lança sombras sobre o nexo causal, especialmente porque o comportamento das máquinas, muitas vezes, transcende a previsibilidade dos próprios programadores. Assim, desponta uma nebulosidade que desafia o arcabouço jurídico clássico e a segurança jurídica pretendida.

Embora instrumentos normativos como o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados constituam avanços inquestionáveis na proteção de dados, seu alcance é limitado frente às especificidades da inteligência artificial. As referidas legislações, ainda que orientadas por princípios gerais de transparência e responsabilidade, não englobam, adequadamente, a autonomia operacional dos sistemas inteligentes. Como evidenciado no caso TikTok, a ausência de uma base protetiva que aborde, precisamente, a opacidade algorítmica e o risco inerente ao uso de IA resulta em falhas que comprometem a proteção dos titulares de dados e a efetividade das sanções impostas.

Neste caminhar, o julgamento analisado revelou um paradoxo inerente ao cenário jurídico atual: embora a condenação da empresa tenha sido viabilizada pelo arcabouço protetivo vigente, persistem dúvidas quanto à origem das irregularidades e às estratégias eficazes para evitar sua repetição. O panorama ressalta a imperiosa necessidade de uma legislação específica, apta a promover transparência algorítmica e estabelecer, de forma rigorosa, as responsabilidades de todos os atores envolvidos, desde desenvolvedores, operadores e controladores até, em certos casos, usuários finais. Sem tal avanço, o ordenamento jurídico permanece reativo, limitado a sancionar condutas após a ocorrência do dano, ao invés de prevenir práticas lesivas.

A experiência europeia, consolidada na promulgação do primeiro marco regulatório de inteligência artificial em 2023, surge como uma referência relevante. Tal legislação institui categorias de risco e regimes de responsabilidade, buscando equilibrar inovação tecnológica e salvaguarda de direitos fundamentais. Em contrapartida, o Projeto de Lei 21/2020, atualmente em tramitação no Brasil, ao adotar o regime subjetivo de responsabilidade, levanta questionamentos acerca da capacidade em responder aos desafios impostos pelas inteligências artificiais, afinal, a escolha normativa parece desconsiderar aspectos fundamentais, como a vulnerabilidade dos titulares de dados e a multiplicidade de agentes envolvidos.

Portanto, observa-se a premente necessidade de um modelo normativo que ultrapasse a fragmentação de soluções e os enfoques restritos a regimes específicos de responsabilidade, reconhecendo a intricada natureza das IA´s. Diante da sofisticação inerente a esses sistemas, a regulação deve articular princípios éticos e técnicos de forma integrada, abrangendo aspectos como transparência algorítmica, supervisão permanente e critérios objetivos para a definição de responsabilidades. Mais do que uma exigência legislativa, tal abordagem configura-se como um imperativo civilizatório, reafirmando o compromisso do ordenamento jurídico com a preservação da dignidade da pessoa humana e a promoção da segurança jurídica, em um cenário tecnológico marcado por constantes evoluções.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD abre processo sancionador e emite determinações ao TikTok**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-processo-sancionador-e-emite-determinacoes-ao-tiktok. Acesso em: 25 nov. 2024.

AMOROZO, M. **Congresso tem pelo menos 46 projetos de lei para regulamentar do uso de inteligência artificial**. Disponível em: <https://www.cnnbrasil.com.br/politica/congresso-tem-pelo-menos-46-projetos-de-lei-para-regulamentar-do-uso-de-inteligencia-artificial>. Acesso em: 16 out. 2024.

ARÁBIA Saudita torna-se o primeiro país a conceder cidadania para um robô. **Revista Galileu**, 26 out. 2017. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2017/10/arabia-saudita-torna-se-primeiro-pais-conceder-cidadania-para-um-robo.html. Acesso em: 26 nov. 2024.

BARBOSA, Mafalda Miranda et al. **Direito Digital e Inteligência Artificial**. [S.l.]: Editora Foco, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro, RJ: GEN, Editora Forense, 2019.

BRASIL. Congresso. Câmara dos Deputados. **Projeto de Lei nº 21/2020**. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928&filename=PL%2021/2020. Acesso em: 10 set. 2024.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 10 set. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 10 set. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 set. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 set. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. **Manual de proteção de dados pessoais para o consumidor**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 17 nov. 2024.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 10. ed. revista e ampliada. São Paulo: Editora Atlas, 2012.

COHEN, Julie E. ***Examined lives: informational privacy and the subject as object***. *Stanford Law Review*, v. 52, p. 1376, 2000.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Inteligência artificial - Portal CNJ**. Disponível em: https://www.cnj.jus.br/sistemas/plataforma-sinapses/inteligencia-artificial. Acesso em: 10 out. 2024.

COPPIN, Ben. **Inteligência artificial**. São Paulo: Grupo GEN, 2010.

DIGNUM, V. ***Responsible Artificial Intelligence - How to Develop and Use AI in a Responsible Way***. *Artificial Intelligence: Foundations, Theory, and Algorithms*. *Springer*, 2019.

DOMINGOS, Pedro. **O Algoritmo Mestre: como a busca pelo algoritmo de *machine learning* definitivo recriará nosso mundo**. São Paulo: Novatec, 2017.

DONEDA, D. C. M.; MENDES, L. S.; PEREIRA DE SOUZA, C. A.; GOMES DE ANDRADE, N. N. M. B. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal**. *Pensar - Revista de Ciências Jurídicas*, v. 23, n. 4, 2018. Disponível em: https://doi.org/10.5020/2317-2150.2018.8257. Acesso em: 10 out. 2024.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Rev. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019.

ELIAS, Paulo Sá. **Algoritmos, Inteligência Artificial e o direito**. [S.l.]: Consultor Jurídico, Disponível em: https://www.conjur.com.br/wp-content/uploads/2023/09/algoritmos-inteligencia-artificial.pdf. Acesso em: 08 out. 2024.

FARIA, Edimur Ferreira de; DAMASCENO, Luiza Mascarenhas. **A Indústria 4.0 e o futuro da prática jurídica no século XXI**. Revista dos Tribunais, São Paulo, v. 1003, p. 239-261, mai./jun. 2019.

FERRAZ JÚNIOR, T. S. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 88, p. 439-459, 1 jan. 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 14 nov. 2024.

FOLHA DE S. PAULO. **O que é inteligência artificial e como ela funciona?**. Disponível em: https://www1.folha.uol.com.br/tec/2022/05/o-que-e-inteligencia-artificial-e-como-ela-funciona.shtml. Acesso em: 10 out. 2024.

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 23-52.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil: responsabilidade civil**. 10. ed. revista, atualizada e ampliada. São Paulo: Saraiva, 2012.

GETPRIVACY. **O que é a ANPD e quais são as suas funções?** Disponível em: https://getprivacy.com.br/anpd-o-que-e/. Acesso em: 18 nov. 2024.

GOMES, Sérgio Tenreiro. **Inteligência artificial e o direito: uma introdução às questões éticas e jurídicas**. Revista Jurídica Luso-Brasileira, v. 5, n. 6, p. 473-514, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf. Acesso em: 22 nov. 2024.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Parte Geral**. Vol. 1. 12. ed. São Paulo: Saraiva, 2012.

HARARI, Yuval Noah. **21 Lições para o Século 21**. Tradução de Paulo Geiger. São Paulo: Companhia das Letras, 2018. p. 107.

ITSRIO. **A Nova Lei Geral de Proteção de Dados: primeiras impressões**. Realização de Danilo Doneda e Laura Schertel. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2018. (103 min.), online, son., color. Aula 1 - A Nova Lei Geral de Proteção de Dados.

LEE, Kai-Fu. **Inteligência Artificial: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos**; tradução Marcelo Barbão – 1. Ed - Rio de Janeiro: Globo Livros, 2019.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011, p. 402.

LIMA, Alvino. **Da culpa ao risco**. São Paulo: Revista dos Tribunais, 1938, p. 31.

LIMA, Isaías. **Inteligência Artificial**. São Paulo: Grupo GEN, 2014, p. 4.

LÔBO, Paulo G. **Responsabilidade civil e inteligência artificial: uma análise à luz do direito civil brasileiro**. Revista Brasileira de Direito Civil, v. 31, p. 123–150, 2022.

Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584/425. Acesso em: 22 nov. 2024.

MIRAGEM, Bruno J. **Responsabilidade civil por danos causados pela utilização de inteligência artificial: desafios e perspectivas no ordenamento jurídico brasileiro**. Revista Brasileira de Direito Civil, v. 29, p. 43–72, 2021.

MULHOLLAND, Caitlin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. Revista Jur. Puc. Rio, 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em 24 nov. 2024.

GARCIA, Bruna Pinotti. **Inteligência artificial e proteção de dados: sobre a autodeterminação informativa e a manipulação informacional por *machine learning***. Revista Multidisciplinar Humanidades e Tecnologias (Finom), Patos de Minas, v. 26, n. 1, p. 162-186, 20 jul. 2020.

PARLAMENTO EUROPEU. **Lei da UE sobre IA: primeira regulamentação de inteligência artificial.** Disponível em: https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial. Acesso em: 14 out. 2024.

PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. 12. ed. Rio de Janeiro: Forense, 2018.

PEREIRA, Laura Schertel Ferreira Mendes. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental**. Brasília: IDP, 2017.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. **A responsabilidade civil pelos atos autônomos da Inteligência Artificial: notas iniciais sobre a resolução do Parlamento Europeu**. In: BARBOSA, Mafalda Miranda et al. (Coord.). **Direito digital e inteligência artificial: diálogos entre Brasil e Europa**. São Paulo: Editora Foco, 2021. p. 334.

RODOTÀ, Stefano. **A vida na sociedade da vigilância. A privacidade hoje**. Trad. Danilo Doneda e Laura Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 111-139.

SENADO FEDERAL. **Comissões Especiais, Temporárias e Parlamentares de Inquérito. Relatório Final: Comissão de juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil**. Brasília, DF: Senado Federal, 2022. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relatório_final_CJSUBIA.pdf. Acesso em: 20 out. 2024.

SERPRO. **Princípios da LGPD**. Disponível em: https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd. Acesso em: 14 nov. 2024.

SOUZA, Anna Beatriz Rodrigues. **Direito à privacidade na era da inteligência artificial: uma análise da proteção de dados pessoais frente à necessidade de uso destes pelas IAs**.

Revista de Direito Civil Contemporâneo, v. 27, n. 2, p. 155-180, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506. Acesso em: 20 nov. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA**. Dano moral coletivo: como o STJ interpreta a ofensa que atinge valores de toda a comunidade.** Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/16062024-Dano-moral-coletivo-como-o-STJ-interpreta-a-ofensa-que-atinge-valores-de-toda-a-comunidade.aspx. Acesso em: 25 nov. 2024.

TARTUCE, Flávio. **Manual de Direito Civil: Volume Único**. 5. ed. São Paulo: Método, 2015.

TEPEDINO, Gustavo; SILVA, Ricardo da Guia. **Desafios da inteligência artificial em matéria de responsabilidade civil**. Revista Brasileira de Direito Civil, v. 21, n. 3, p. 61-94, 2019. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/465/308. Acesso em: 01 nov. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Interface entre a LGPD e a área pública e privada**. Cadernos Jurídicos da Escola Paulista da Magistratura, v. II, n. 1, 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621. Acesso em: 17 nov. 2024.

ZIMPRICH, Stephan. *The EU – **AI Regulation – Part 1: Overview and structure**. Fieldfisher,* 24 ago. 2021. Disponível em: https://www.fieldfisher.com/en/insights/the-eu-ai-regulation-part-1. Acesso em: 14 nov. 2024.

ANEXO A – SENTENÇA ANALISADA NA MONOGRAFIA

CLASSE PROCESSUAL: AÇÃO CIVIL COLETIVA
PROCESSO: 0816292-73.2020.8.10.0001
AUTOR: INSTITUTO BRASILEIRO DE ESTUDO E DEFESA DAS RELAÇÕES DE CONSUMO
RÉU: BYTEDANCE BRASIL TECNOLOGIA LTDA.

SENTENÇA

Trata-se de Ação Civil Coletiva de Consumo por Prática Abusiva c/c Pedido de Tutela de Urgência Antecipada proposta pelo Instituto Brasileiro de Defesa das Relações de Consumo – IBEDEC/MA em face de BYTEDANCE BRASIL TECNOLOGIA LTDA (TikTok).

O autor narra que o réu, em meados de 2020, contrariou a proteção legal dada aos consumidores quanto aos direitos fundamentais à privacidade, à intimidade, à honra e à imagem, bem como ao coletar indiscriminadamente dados pessoais (biometria facial) dos usuários, armazenando e compartilhando os referidos dados sem o consentimento prévio dos usuários, havendo, portanto, a configuração de práticas ilícitas e abusivas, tendo em vista o vazamento de dados pessoais de consumidores, contrariando flagrantemente os deveres de informação e transparência.

Aduz o autor que o réu também se omite quanto ao que faz com os dados capturados, a exemplo de quem teria acesso a estes dados e por quanto tempo os mesmos seriam armazenados e compartilhados.

O instituto autor alega ter recebido diversas reclamações dos usuários tendo em vista que o réu nocivamente implementou no aplicativo uma ferramenta de inteligência artificial que automaticamente digitaliza o rosto dos usuários, visando a captura, armazenamento e compartilhamento de dados, sem o devido consentimento dos usuários. Soma-se a este fato a vagueza dos seus “termos de uso” e “política de privacidade”.

Em suma, alega o autor que os recursos lúdicos do aplicativo usurpam a privacidade dos usuários. E, no mesmo vetor, o aplicativo verifica a geometria facial dos indivíduos antes de executar um algoritmo, capturando seus dados pessoais indevidamente e sem autorização.

O autor afirma, ainda, que o réu desrespeita em diversos sentidos as normas legais de proteção à privacidade de seus usuários, expondo-os a riscos maiores, como fraudes e roubos de dados.

Quanto aos pedidos principais, o IBEDEC requer a condenação do réu ao pagamento de indenização por danos morais coletivos no valor de R$ 23.000.000,00 (vinte e três milhões de reais), a ser revertido em favor do Fundo Estadual de Proteção e Defesa dos Direitos do Consumidor – FPDC, criado pela Lei Estadual nº 8.044, de 19 de dezembro de 2003. Requerendo, ainda, a condenação do demandado a pagar a cada consumidor lesado indenização por danos morais no valor de R$ 10.000,00 (dez mil reais).

Formula, por fim, como pedido acessório a condenação do réu: a divulgação de sua condenação nas mídias sociais, no prazo de 05 (cinco) dias, a contar do trânsito em julgado de eventual sentença de procedência, para que os consumidores possam tomar ciência da decisão proferida, informando-os quanto aos direitos protegidos, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais), sem prejuízo do disposto no art. 84 § 5º do CDC.

Juntada de contestação aos autos (id 37320715), em que se alega, preliminarmente, ilegitimidade ativa, ausência de autorização expressa e específica para ajuizamento da ação, falta de interesse de agir (tendo em vista premissa claramente equivocada), ilegitimidade passiva da BYTEDANCE BRASIL TECNOLOGIA LTDA. No mérito, sustenta que a ação deve ter seus pedidos rejeitados em todos os seus termos, argumentando, ausência de violação do Código de Defesa do Consumidor, inexistência de tratamento de dados biométricos faciais (*landmarking*).

Em réplica o autor reitera os termos da petição inicial (id 38453201), notadamente sustentando sua legitimidade ativa, e no mérito a condenação do réu em dano moral coletivo pela prática de conduta ilícita de coleta ilegal de dados.

Arguição de suspeição com pedido de efeito suspensivo (id 40673405), porém julgada improcedente (id 62987046).

Não concedida a tutela de urgência (id 62987046).

Agravo de instrumento interposto por IBEDEC (id 65703864), porém negado provimento (id 72524974).

Tréplica juntada aos autos ratificando as argumentações dispostas na contestação (id 66257601).

Devidamente intimadas, as partes requereram o julgamento antecipado da lide (id 64580161).

Instado a manifestar-se, o Ministério Público Estadual pugnou pela improcedência da ação (id 79203142).

Vieram-me os autos conclusos para julgamento.

É o Relatório.

FUNDAMENTAÇÃO:

Das Preliminares:

Ilegitimidade Ativa:

A autora possui legitimidade para propositura de ações civis públicas em defesa de direitos individuais homogêneos e difusos de consumidores de serviços de internet, com fundamento no art. 82, IV, do CDC e art. 5º, V, da Lei nº 7.347/1985.

Como já decidiu o STJ, "o fato do serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração' contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor" (REsp n. 1.192.208/MG, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 12/6/2012, DJe de 2/8/2012).

No presente caso, o IBEDEC atua tanto em defesa de direitos individuais homogêneos quanto de interesses difusos. Os direitos à privacidade, à proteção dos dados, a um ambiente seguro na internet (causas de pedir da presente ação) podem ser objeto tanto de tutela individual quanto coletiva, a depender da relação jurídica a que se refere a pretensão trazida a Juízo.

Nesta ação, segundo os fatos e fundamentos jurídicos que compõem a petição inicial, alega-se que houve violação de direitos individuais dos usuários do TikTok que tiveram, supostamente, indevidamente coletados dados de biometria facial, bem como que o fato tido por ilegal afetou o direito difuso a um ambiente de navegação seguro na internet.

Como há origem comum na suposta lesão aos direitos individuais, qual seja, captura de dados pessoais de usuários sem o necessário consentimento, configurada está a homogeneidade presente no art. 81, parágrafo único, III, do CDC, sendo irrelevante se o direito é disponível ou não.

Como a associação atua nos presentes autos em regime de substituição processual, é dispensada a autorização assemblear, sendo suficiente a demonstração de pertinência entre seus objetivos e os direitos defendidos nesta ação, o que ficou demonstrado pela juntada de seu estatuto.

O tema tem relação com a eficácia subjetiva da coisa julgada em ações coletivas, cuja discussão gira em torno do regime de atuação das associações: se agem por representação ou por legitimação extraordinária na qualidade de substitutas processuais.

Essa questão foi submetida ao STF no RE 612.043/PR, oportunidade em que a Corte Suprema fixou a seguinte tese:

> A eficácia subjetiva da coisa julgada formada a partir de ação coletiva, de rito ordinário, ajuizada por associação civil na defesa de interesses dos associados, somente alcança os filiados, residentes no âmbito da jurisdição do órgão julgador, que o fossem em momento anterior ou até a data da propositura da demanda, constantes da relação jurídica juntada à inicial do processo de conhecimento.

Cuidou a Suprema Corte, no embargos de declaração opostos contra o julgamento, em decisão do Ministro Marco Aurélio, de esclarecer que o entendimento supracitado se restringia às ações de rito ordinário, não se aplicando às ações civis públicas e ações coletivas de consumo, que possuem rito próprio.

Essa orientação foi seguida pelo Superior Tribunal de Justiça que, em julgados mais recentes, dispensa a autorização assemblear ou individualizada dos associados para propositura de ações em defesa de direitos transindividuais:

> AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. PROCESSUAL CIVIL. AÇÃO COLETIVA. ASSOCIAÇÃO. LEGITIMIDADE ATIVA. EXPRESSA AUTORIZAÇÃO ASSEMBLEAR. PRESCINDIBILIDADE. PRECEDENTES DESTA CORTE. AGRAVO DESPROVIDO. 1. Não se aplica ao caso vertente o entendimento sedimentado pelo STF no RE n. 573.232/SC e no RE n. 612.043/PR, pois a tese firmada nos referidos precedentes vinculantes não se aplica às ações coletivas de consumo ou quaisquer outras demandas que versem sobre direitos individuais homogêneos. Ademais, a Suprema Corte acolheu os embargos de declaração no RE n. 612.043/PR para esclarecer que o entendimento nele firmado alcança tão somente as ações coletivas submetidas ao rito ordinário. 2. Consoante a jurisprudência do STJ, "por se tratar do regime de substituição processual, a autorização para a defesa do interesse coletivo em sentido amplo é estabelecida na definição dos objetivos institucionais, no próprio ato de criação da associação, sendo desnecessária nova autorização ou deliberação assemblear" (REsp 1.649.087/RS, Relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 02/10/2018, DJe 04/10/2018). 3. Agravo interno desprovido. (AgInt no AREsp n. 1.441.016/RS, relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 27/5/2019, DJe de 31/5/2019.)

> RECURSO ESPECIAL. PROCESSO CIVIL COLETIVO. LEGITIMIDADE ATIVA DAS ASSOCIAÇÕES. ATUAÇÃO COMO REPRESENTANTE E SUBSTITUTA PROCESSUAL. RE n. 573.232/SC. AÇÃO COLETIVA ORDINÁRIA. REPRESENTAÇÃO. NECESSIDADE DE AUTORIZAÇÃO ESPECÍFICA. AÇÃO CIVIL PÚBLICA. DIREITOS INDIVIDUAIS HOMOGÊNEOS. SUBSTITUIÇÃO PROCESSUAL. DESNECESSIDADE DE AUTORIZAÇÃO NOMINAL. TARIFA POR LIQUIDAÇÃO ANTECIPADA. POSSIBILIDADE DA COBRANÇA ATÉ 10/12/2007, COM INFORMAÇÃO EXPRESSA. VERIFICAÇÃO EM LIQUIDAÇÃO. [...] Na presente demanda, a atuação da entidade autora deu-se, de forma inequívoca, no campo da substituição processual, sendo desnecessária a apresentação nominal do rol de seus filiados para ajuizamento da ação. 8. Nesses termos, tem-se que as associações instituídas na forma do art. 82, IV, do CDC estão legitimadas para propositura de ação civil pública em defesa de interesses individuais homogêneos, não necessitando para tanto de autorização dos associados. Por se tratar do regime de substituição processual, a autorização para a defesa do interesse coletivo em sentido amplo é estabelecida na definição dos objetivos institucionais, no próprio ato de criação da associação, não sendo necessária nova autorização ou deliberação assemblear. (…) (STJ - REsp: 1325857 RS 2011/0236589-7, Relator: Ministro LUÍS FELIPE SALOMÃO, Data de Julgamento: 30/11/2021, S2 - SEGUNDA SEÇÃO, Data de Publicação: DJe 01/02/2022).

REJEITO, portanto, a preliminar de ilegitimidade ativa.

Ilegitimidade Passiva:

O art. 75, X, do CPC, prevê que “serão representados em juízo, ativa e passivamente, a pessoa jurídica estrangeira, pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil.”. Além disso, o §3º dispõe, ainda, que o gerente de filial ou agência presume-se autorizado pela pessoa jurídica estrangeira a receber citação para qualquer processo.

Assim, mesmo que a pessoa jurídica estrangeira opere no Brasil por meio de uma empresa que não tenha sido oficialmente estabelecida como sua filial ou agência, isso não impede que sua citação seja regularmente realizada por meio dela.

O Superior Tribunal de Justiça já se manifestou nesse sentido, firmando importante precedente:

> Com o fim de facilitar a comunicação dos atos processuais às pessoas jurídicas estrangeiras no Brasil, o art. 75, X, do CPC prevê que a pessoa jurídica estrangeira é representada em juízo 'pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil' e o parágrafo 3º do mesmo artigo estabelece que o 'gerente de filial ou agência presume-se autorizado pela pessoa jurídica estrangeira a receber citação para qualquer processo'. Considerando-se que a finalidade destes dispositivos legais é facilitar a citação da pessoa jurídica estrangeira no Brasil, tem-se que as expressões "filial, agência ou sucursal" não devem ser interpretadas de forma restritiva, de modo que o fato de a pessoa jurídica estrangeira atuar no Brasil por meio de empresa que não tenha sido formalmente constituída como sua filial ou agência não impede que por meio dela seja regularmente efetuada sua citação." (HDE 410/EX, Rel. Ministro BENEDITO GONÇALVES, CORTE ESPECIAL, julgado em 20/11/2019, DJe 26/11/2019).

No presente caso, a BYTEDANCE BRASIL é a empresa por meio da qual o TikTok atua no país, de modo que possui legitimidade para figurar no polo passivo da ação.

REJEITO a preliminar de ilegitimidade passiva arguida pelo Réu.

Da alegação de ausência de interesse processual e de inépcia da petição inicial.

Para o exame da presença das condições da ação adotou-se a teoria da asserção (STJ: AgRg no AREsp 205.533/SP; AgRg no AREsp 53.146/SP).

Segundo a teoria da asserção, as questões relacionadas às condições da ação, como a legitimidade e o interesse processual, são aferidas à luz do que o autor afirma na petição inicial, adstritas ao exame da possibilidade, em tese, da existência do vínculo jurídico-obrigacional entre as partes, e não do direito provado.

No caso em análise, o interesse processual está presente, uma vez que é necessário investigar a responsabilidade do Réu diante das alegadas violações à privacidade, intimidade, honra, imagem e direitos dos consumidores, resultantes da suposta coleta de dados pessoais em desacordo com a lei. Além disso, a ação civil pública é o meio adequado para defender direitos coletivos, sendo útil e necessário para a tutela pretendida na inicial, considerando que há resistência por parte do Réu às pretensões apresentadas.

Não há necessidade que a inicial seja instruída com provas robustas do alegado (embora o autor tenha anexado à petição inicial documentos com a finalidade de comprovar suas alegações), pois, conforme já consignado, a análise sobre a presença das condições da ação é feita abstratamente.

Há nítida alegação de violação de direito difuso e direito individual homogêneo, porquanto há um fato de origem comum do qual decorrem, segundo alegado, inúmeras violações de direitos individuais. Tal circunstância autoriza a sua defesa por meio de tutela coletiva. Ademais, tendo em vista que os pedidos formulados em ações coletivas tendem a ser mais genéricos (CDC, art. 95), entendo que ficaram preenchidos os requisitos do art. 319 do CPC.

REJEITO a preliminar de ausência de interesse processual e inépcia da petição inicial.

Do Mérito:

No ordenamento jurídico brasileiro, a proteção à privacidade e à proteção de dados encontra amparo tanto na Constituição Federal quanto em legislações infraconstitucionais, como o Marco Civil da Internet (Lei 12.965/2014). O artigo 5º, inciso X, da Constituição Federal de 1988, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo o direito à indenização pelo dano material ou moral decorrente de sua violação. Além disso, a Emenda Constitucional nº 115, de 2022, incluiu o inciso LXXIX ao mesmo artigo, assegurando o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A proteção de dados pessoais encontra respaldo constitucional, derivando dos direitos da personalidade, em especial do direito à privacidade e à autodeterminação informativa. Tal prerrogativa impõe que o tratamento e a manipulação de dados pessoais, por estarem relacionados à identificação de pessoa natural, estejam submetidos aos limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII).

Assim, a utilização de dados pessoais deve vincular-se a uma finalidade legítima e específica, devendo observar os princípios da necessidade, adequação e proporcionalidade.

Essa proteção constitucional se alinha com os princípios estabelecidos na Carta dos Direitos Fundamentais da União Europeia, em seu artigo 8º, que dispõe sobre a proteção de dados pessoais. Tal dispositivo estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito, determinando que o tratamento desses dados deve ser feito de forma justa, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Ademais, estabelece o direito de acesso e retificação desses dados, bem como a fiscalização por uma autoridade independente.

No cenário jurídico internacional, a proteção de dados pessoais é reconhecida como um direito fundamental, o que se reflete na legislação de diversos países, bem como em tratados e convenções internacionais. A União Europeia, por exemplo, possui o Regulamento Geral de Proteção de Dados (GDPR ou RGPD), que estabelece diretrizes rigorosas para o tratamento de dados pessoais. Essa proteção internacional se relaciona diretamente com a garantia constitucional brasileira, reforçando a importância e a necessidade de proteção da privacidade e dos dados pessoais dos cidadãos, inclusive no ambiente digital.

No contexto nacional, o Marco Civil da Internet estabelece princípios fundamentais para a utilização da internet no Brasil. O artigo 3º, inciso II, determina a proteção da privacidade, enquanto o inciso III assegura a proteção dos dados pessoais, na forma da lei. Além disso, o artigo 7º da referida lei garante ao usuário direitos como a inviolabilidade da intimidade e da vida privada, o sigilo do fluxo de comunicações pela internet e o não fornecimento a terceiros de seus dados pessoais sem consentimento livre, expresso e informado.

Pela pertinência, transcrevo os mencionados dispositivos:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (...) II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei; (...)
>
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> (...) VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; (Lei nº 12.695/2014).

A mencionada lei ainda determina que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (art. 11).

Esses dispositivos do Marco Civil da Internet, ao estabelecerem a proteção da privacidade e dos dados pessoais, estão em consonância com o direito à autodeterminação informativa, que encontra suas bases no direito constitucional à privacidade e à proteção de dados. Dada sua densidade normativa, em 2018, foi positivado na Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que, ao reconhecer a importância da autodeterminação informativa, reforça a proteção dos dados pessoais como um elemento essencial para a preservação da privacidade e da liberdade individual.

A autodeterminação informativa compreende a capacidade do indivíduo de controlar suas próprias informações, decidindo sobre sua coleta, utilização e compartilhamento por terceiros.

Dessa forma, o arcabouço jurídico brasileiro solidifica a proteção do direito fundamental à privacidade e à proteção de dados no ambiente da internet. Assim, a coleta, uso e o tratamento indevido de dados de usuários, sem o necessário livre consentimento, configura violação dessas normas.

Na hipótese dos autos, verifico que o réu, em sua defesa, argumentou ausência de violações à boa-fé, informação, lealdade e transparência, afirmando que não há na plataforma do aplicativo TikTok qualquer dispositivo que proceda com a coleta dos dados dos usuários a partir da biometria facial. Aduziu, ainda, que a plataforma não permite o compartilhamento de dados com terceiros, conforme alega o instituto autor.

As evidências constantes dos autos, entretanto, indicam o contrário.

Conforme documentos juntados pelo autor, o réu firmou acordo com o Governo dos Estados Unidos, no valor de US$ 92 milhões de dólares, para pôr fim a diversas demandas judiciais que tratavam de violações à privacidade de seus usuários, dentre as quais a captura de dados de biometria facial.

Adicionalmente, consta de sítio eletrônico na internet (https://time.com/6071773/tiktokfaceprints-voiceprints-privacy/) que, em junho de 2021, o TikTok promoveu atualização em sua política de privacidade para incluir nela a possibilidade de coleta automática de dados da face e de voz dos seus usuários (*faceprints and voiceprints*),

deixando claro, assim, o que já se evidenciou que fazia no passado, mas à revelia do consentimento de seus clientes.

Apesar da ré tentar diferenciar em sua contestação de que modo ocorre o tratamento de dados da face de seus usuários, distinguindo o que seria detecção facial/reconhecimento facial, entendo que todas as imagens faciais capturadas pelo aplicativo devem ser tratadas como dados biométricos, uma vez que, do ponto de vista do usuários e de autoridades reguladoras, há grande dificuldade em se distinguir tais aspectos de abordagem, bem como determinar qual o uso realmente feito pelo provedor. E, de fato, independentemente do uso que seja feito das imagens capturadas, elas podem identificar uma pessoa.

A coleta e armazenamento de dados biométricos foi ilegal, porque não houve consentimento livre, expresso e informado nesse sentido (Lei nº 12.965/2014, art. 7º, IX; Lei nº 13.709/2018, art. 5º, II e X c/c art. 11, I).

Considerando a relação entre os usuários e os provedores de serviços de internet como uma relação de consumo, nos termos do Código de Defesa do Consumidor (CDC), delineada pelo artigo 2º que define consumidor como toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final, inclusive equiparando-se a coletividade de pessoas que haja intervindo nas relações de consumo, e pelo artigo 3º que define fornecedor como toda pessoa física ou jurídica que desenvolve atividade de prestação de serviços, produção, montagem, criação, distribuição ou comercialização de produtos ou serviços, é imperativo atentar aos dispositivos legais em questão.

A jurisprudência consolidada do Superior Tribunal de Justiça (STJ) tem firmado o entendimento de que o fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não elide a caracterização da relação de consumo, conforme visto no REsp n. 1.192.208/MG, julgado pela Terceira Turma em 12/06/2012, DJe de 02/8/2012. Tal entendimento ressalta que o termo "mediante remuneração" contido no art. 3º, §2º, do CDC, deve ser interpretado amplamente, abrangendo inclusive o ganho indireto do fornecedor.

Assim, uma vez reconhecida a relação de consumo entre os usuários e os provedores de serviços de internet, mesmo quando o serviço é oferecido de forma gratuita, é possível dizer que a captura de biometria facial de seus usuários, sem consentimento, configura uma falha na prestação do serviço, nos termos do artigo 14 do CDC.

Nesse contexto, os provedores de aplicativos de internet podem ser responsabilizados pela reparação dos danos individualmente suportados pelos usuários, bem como pelo dano moral coletivo decorrente de sua conduta.

No presente caso, entendo que ficaram configurados todos os elementos necessários para responsabilização do TikTok, em razão da indevida coleta de dados biométricos de seus usuários, ou seja, estão presentes a conduta, o nexo de causalidade e o dano. Na hipótese, não cabe discutir dolo ou culpa, pois, configurada a relação de consumo, a responsabilidade é objetiva (CDC, art. 14, §3º).

Quanto aos danos, considero demonstrados tanto danos morais individuais quanto o dano moral coletivo.

O dano moral individual, geralmente, demanda a comprovação de prejuízo efetivo, sendo assim, eminentemente subjetivo. Para sua configuração, é necessário demonstrar a existência de dano, lesão, angústia, dor, humilhação ou sofrimento pessoal do prejudicado. Contudo, em certas circunstâncias, o Superior Tribunal de Justiça tem admitido o reconhecimento do dano moral presumido (*in re ipsa*).

Cito, por exemplo, o seguinte julgado relatado pela Ministra Nancy Andrighi, no qual se reconheceu que o dano moral é presumido na situação em que ocorre o compartilhamento de dados pessoais mantidos em banco de dados por terceiros sem autorização do titular dos dados.

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado - quando suficiente para a manutenção das conclusões do acórdão recorrido - impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema *credit scoring*, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência - CDC e Lei 12.414/2011 - dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da

> Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. (REsp n. 1.758.799/MG, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 12/11/2019, DJe de 19/11/2019.)

É evidente, portanto, que no caso de captura não autorizada de biometria facial do usuário (dado sensível, conforme art. 5º, II, da LGPD), sem a autorização do titular, o dano moral é presumido. Isso se justifica pelo fato de que, no contexto contemporâneo, a proteção da privacidade e dos dados pessoais é um direito fundamental cada vez mais relevante, assim tratado tanto na legislação quanto na jurisprudência.

Por outro lado, não seria razoável exigir do titular dos dados compartilhados indevidamente que ele demonstrasse o abalo moral decorrente, uma vez que muitas vezes não é dado a ele conhecer para que fins estão sendo utilizados seus dados, especialmente no caso concreto, em que a captura dos dados ocorreu de forma sorrateira, à revelia do usuário.

A hipótese ora retratada neste processo se distingue daquela analisada pelo STJ no AREsp n. 2.130.619/SP, visto que naquele caso o STJ afastou a possibilidade de reconhecimento de dano moral presumido na hipótese de vazamento de dados pessoais.

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. *In casu*, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp

> 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido. (AREsp n. 2.130.619/SP, relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.)

No presente caso, estabelece-se que a mera coleta não autorizada de dados biométricos (sensíveis) causa dano moral.

Portanto, diante da violação do dever de informação e do direito à autodeterminação informativa do titular dos dados, o dano moral é presumido, pois a coleta não autorizada de dados biométricos gera, por si só, um abalo à dignidade e à intimidade do indivíduo. Assim, é justificável reconhecer o dano moral *in re ipsa* em casos de coleta indevida de dados biométricos, como no presente caso.

Quanto ao dano moral coletivo, enquanto categoria autônoma de dano, caracteriza-se por lesão grave, injusta e intolerável a valores e interesses fundamentais da sociedade, independentemente da comprovação de prejuízos concretos ou de efetivo abalo moral, conforme pacificado pelo STJ. Nesse sentido:

> RECURSO ESPECIAL. AÇÃO CIVIL PÚBLICA. DANO MORAL COLETIVO. DIREITOS INDIVIDUAIS HOMOGÊNEOS. IMPOSSIBILIDADE. 1. O dano moral coletivo é aferível in re ipsa, ou seja, sua configuração decorre da mera constatação da prática de conduta ilícita que, de maneira injusta e intolerável, viole direitos de conteúdo extrapatrimonial da coletividade, revelando-se despicienda a demonstração de prejuízos concretos ou de efetivo abalo moral. Precedentes. 2. Independentemente do número de pessoas concretamente atingidas pela lesão em certo período, o dano moral coletivo deve ser ignóbil e significativo, afetando de forma inescusável e intolerável os valores e interesses coletivos fundamentais. 3. O dano moral coletivo é essencialmente transindividual, de natureza coletiva típica, tendo como destinação os interesses difusos e coletivos, não se compatibilizando com a tutela de direitos individuais homogêneos. 4. A condenação em danos morais coletivos tem natureza eminentemente sancionatória, com parcela pecuniária arbitrada em prol de um fundo criado pelo art. 13 da LACP - *fluid recovery* - , ao passo que os danos morais individuais homogêneos, em que os valores destinam-se às vítimas, buscam uma condenação genérica, seguindo para posterior liquidação prevista nos arts. 97 a 100 do CDC. 5. Recurso especial a que se nega provimento. (REsp n. 1.610.821/RJ, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 15/12/2020, DJe de 26/2/2021.)

Logo, para a demonstração desse tipo de dano, é suficiente a constatação da prática de conduta ilícita que viole direitos de conteúdo extrapatrimonial da coletividade, dispensando-se a necessidade de comprovação de prejuízos concretos.

No caso em análise, ocorreu a coleta de dados biométricos de usuários, à revelia da autorização de seus titulares, o que evidencia uma lesão à confiança nas relações negociais, o que gera transtornos significativos à coletividade.

O fato representa uma violação séria da privacidade e segurança dos usuários. As consequências desse tipo de violação podem ser amplas e duradouras, afetando a confiança no uso de tecnologias e exigindo medidas rigorosas de proteção de dados por parte das autoridades públicas.

Portanto a reparação pelos danos morais coletivos deve ser fixada de modo a desencorajar a reincidência da falta, sem, contudo, propiciar enriquecimento indevido, devendo ser avaliada à luz da proporcionalidade da ofensa (STJ - REsp: 1124471 RJ 2009/0082448-1, Relator: Ministro LUIZ FUX, Data de Julgamento: 17/06/2010, T1 - PRIMEIRA TURMA, Data de Publicação: DJe 01/07/2010; STJ, AgRg no Ag 1.410.038).

Dito isto, é preciso ter em mente que a BYTEDANCE, empresa controladora do TikTok, registrou um lucro operacional de aproximadamente US$ 6 bilhões apenas no primeiro trimestre de 2023, sendo hoje considerada uma das maiores empresas de tecnologia do mundo (https://br.investing.com/news/stock-market-news/dona-do-tiktok-reporta-lucrooperacional-de-us-20-bi-valuation-cai-para-us-220-bi1161922#:~:text=Em%202022%2C%20a%20receita%20da,operacional%20durante%20o%20ano%20todo.).

Nesse cenário, entendo razoável a fixação da quantia devida a título de indenização pelo dano moral coletivo em R$ 23 milhões de reais, valor constante do pedido formulado na petição inicial, tendo em vista a gravidade da conduta da ré, consistente na coleta indiscriminada, não autorizada, de dados sensíveis (biometria facial).

Outrossim, sabendo que cada consumidor individualmente considerado também sofreu dano moral, bem como por entender que deixar a fixação do quantum para eventual liquidação de sentença atenta contra princípios processuais relevantes, especialmente o da efetividade e celeridade, entendo por bem arbitrar a indenização pelo dano moral individual em R$ 500,00 (quinhentos reais) para cada cliente atingido pela coleta de dados biométricos.

Beneficiários desta sentença são todos os usuários do TikTok, no território nacional, que comprovem esta condição até a data da atualização da Política de Dados da plataforma que incluiu a possibilidade de captura de dados biométricos de seus usuários, ou seja, junho de 2021.

DISPOSITIVO

Nos termos do art. 487, I, do CPC, ACOLHO os pedidos formulados pelo IBEDEC em face de BYTEDANCE BRASIL TECNOLOGIA LTDA (TikTok) e, por conseguinte, CONDENO a ré ao pagamento de:

i) R$ 23 milhões de reais, a título de dano moral coletivo;

ii) R$ 500,00, a título de dano moral individual para cada usuário do TikTok, no território nacional, que comprove esta condição até a data da atualização da Política de Dados da plataforma que incluiu a possibilidade de captura de dados biométricos de seus usuários, ou seja, junho de 2021, observando que a execução deve ocorrer em cumprimento individual de sentença no Juízo competente para processar e julgar demandas individuais.

DETERMINO, ainda, que a ré:

a) Abstenha-se de coletar e compartilhar dados biométricos do usuário sem o necessário consentimento;

b) Explicite ao usuário de que forma o consentimento é obtido no procedimento de adesão ao ecossistema do programa, com exposição das janelas, condições, línguas e caixas de diálogo em que são inseridos os termos deste consentimento;

c) Implemente, de forma destacada, com transparência e clareza, ferramenta operacional para obter o consentimento do usuário da plataforma, oportunizando ao consumidor que autorize ou não a coleta de dados biométricos;

d) Exclua os dados biométricos coletados ilegalmente sem consentimento dos usuários.

CONDENO, por fim, a ré ao pagamento das custas processuais e honorários advocatícios, fixados em 10% do valor da condenação, nos termos do art. 85 do CPC, considerando, em especial, a complexidade da causa e o grau de zelo do profissional, ressaltando o aspecto positivo do manejo da ação coletiva para concretização de valores jurídicos relevantes para sociedade.

PUBLIQUEM. INTIMEM.

São Luís, datado eletronicamente.

Dr. Douglas de Melo Martins

Juiz Titular da Vara de Interesses Difusos e Coletivos