

UNIVERSIDADE FEDERAL DE UBERLÂNDIA - UFU
FACULDADE DE DIREITO “PROFESSOR JACY DE ASSIS” - FADIR
GRADUAÇÃO EM DIREITO

GABRIELA MORAIS SIMÃO DA GAMA
12121DIR052

PRIVACIDADE EMOCIONAL: OS LIMITES DA COLETA DE DADOS SENSÍVEIS
EM PLATAFORMAS DIGITAIS

UBERLÂNDIA - MG

2026

GABRIELA MORAIS SIMÃO DA GAMA

Privacidade emocional: os limites da coleta de dados sensíveis em plataformas digitais

Trabalho de Conclusão de Curso componente ao TCC-2 apresentado à Faculdade de Direito Prof. Jacy de Assis da Universidade Federal de Uberlândia como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientadora: Prof.^a Dra. Keila Pacheco Ferreira

UBERLÂNDIA - MG

2026

Privacidade emocional: os limites da coleta de dados sensíveis em plataformas digitais

Trabalho de conclusão de curso orientado pela Prof.^a Dra. Keila Pacheco Ferreira, apresentado à Faculdade de Direito da Universidade Federal de Uberlândia (UFU), como requisito para obtenção do grau de bacharel em Direito, aprovado pela banca examinadora formada por:

Uberlândia/MG, 02 de julho de 2026.

Prof.^a Dra. Keila Pacheco Ferreira
Orientadora – Professora Doutora na UFU

Prof. Dr. Fernando Rodrigues Martins
Professor Doutor da UFU

Jeová Marques de Oliveira
Mestrando da Faculdade de Direito da UFU

RESUMO

A sociedade contemporânea tem sido profundamente remodelada por uma evolução tecnológica exponencial que direcionou as interações humanas para um fluxo constante e ubíquo de informações. Essa dinâmica estabeleceu uma "economia de vigilância" na qual os dados pessoais tornaram-se a moeda principal, posicionando o cidadão como um mero espectador do processamento de suas próprias informações em uma relação marcadamente assimétrica. A problemática central reside na "datificação" do comportamento humano, que transcende preferências de consumo para abranger a "privacidade emocional", permitindo que plataformas digitais analisem e capitalizem as emoções dos usuários por meio de arquiteturas de decisão complexas e, por vezes, "traíçoeiras". Diante dessa vulnerabilidade, o estudo investiga os limites jurídicos da coleta de dados sensíveis de cunho emocional e a eficácia dos mecanismos de proteção existentes no Brasil. A pesquisa, de natureza qualitativa e baseada em estudo bibliográfico e documental, analisa a aplicabilidade da Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018) e do Marco Civil da Internet (Lei nº 12.965/2014) como instrumentos de preservação da autodeterminação informativa. Discute-se, ainda, o papel regulatório da Autoridade Nacional de Proteção de Dados (ANPD) e os desafios da responsabilidade civil frente ao tratamento irregular desses dados, buscando garantir que o fluxo informacional não seja corrosivo ao livre desenvolvimento da personalidade humana. Por fim, a análise propõe uma reflexão sobre a necessidade de novas interpretações normativas que assegurem a efetividade dos direitos fundamentais na era digital, protegendo a esfera mais íntima do indivíduo contra a manipulação algorítmica.

Palavras-chave: privacidade emocional, LGPD, dados sensíveis, economia de vigilância, autodeterminação informativa, vulnerabilidade digital.

ABSTRACT

Contemporary society has been deeply reshaped by exponential technological evolution, which has directed human interactions toward a constant and ubiquitous flow of information. This dynamic established a "surveillance economy" in which personal data became the primary commodity, positioning citizens as mere spectators of their own information processing within a markedly asymmetric relationship. The central issue lies in the "datafication" of human behavior, which transcends consumption preferences to encompass "emotional privacy," allowing digital platforms to analyze and capitalize on users' emotions through complex and often "treacherous" decision architectures. Given this vulnerability, this study investigates the legal limits of collecting sensitive emotional data and the effectiveness of existing protection mechanisms in Brazil. The research, qualitative in nature and based on bibliographic and documentary studies, analyzes the applicability of the General Data Protection Law (LGPD — Law No. 13.709/2018) and the Marco Civil da Internet (Law No. 12.965/2014) as instruments for preserving informational self-determination. Furthermore, it discusses the regulatory role of the National Data Protection Authority (ANPD) and the challenges of civil liability regarding the irregular processing of such data, seeking to ensure that the informational flow is not corrosive to the free development of the human personality. Finally, the analysis proposes a reflection on the need for new normative interpretations that ensure the effectiveness of fundamental rights in the digital age, protecting the individual's most intimate sphere against algorithmic manipulation.

Keywords: emotional privacy, LGPD, sensitive data, surveillance economy, informational self-determination, digital vulnerability.

SUMÁRIO

INTRODUÇÃO	7
CAPÍTULO 1 - DELIMITAÇÕES CONCEITUAIS E EVOLUÇÃO JURÍDICA.....	9
1.1 O CONCEITO CLÁSSICO DE PRIVACIDADE E O <i>RIGHT TO BE LET ALONE</i>	10
1.2 A AUTODETERMINAÇÃO INFORMATIVA E A PROTEÇÃO DE DADOS PESSOAIS.....	12
1.3 A AUTODETERMINAÇÃO INFORMATIVA E OS SISTEMAS NORMATIVOS DE PROTEÇÃO.....	15
CAPÍTULO 2 – A PRIVACIDADE EMOCIONAL E A COLETA DE DADOS SENSÍVEIS.....	18
2.1 DEFINIÇÃO DE DADOS EMOCIONAIS COMO DADOS SENSÍVEIS.....	18
2.2 ALGORITMOS DE ANÁLISE DE SENTIMENTO E BIOMETRIA COMPORTAMENTAL.....	21
2.3 VULNERABILIDADE DIGITAL E ALGORÍTMICA: A EXPLORAÇÃO DO TITULAR PELOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL.....	22
2.4 A "ARQUITETURA DE ESCOLHA" E A CRISE DO CONSENTIMENTO NAS PLATAFORMAS DIGITAIS.....	27
CAPÍTULO 3 – LIMITES JURÍDICOS E A EFETIVIDADE DA PROTEÇÃO NO BRASIL.....	30
3.1 O PAPEL DA ANPD NA REGULAÇÃO DE TECNOLOGIAS DE RECONHECIMENTO EMOCIONAL.....	31
3.2 A RESPONSABILIDADE CIVIL NO TRATAMENTO IRREGULAR DE DADOS EMOCIONAIS.....	33
3.3 PROPOSTAS PARA O FORTALECIMENTO DA AUTODETERMINAÇÃO INFORMATIVA EMOCIONAL.....	36
CONSIDERAÇÕES FINAIS.....	40
REFERÊNCIAS.....	42

INTRODUÇÃO

A proliferação de plataformas digitais de intermediação social e comercial, especialmente a partir da década de 2010, reconfigurou a relação entre usuários e tratadores de dados, transformando informações pessoais em insumo econômico. Nesse cenário, os dados pessoais deixaram de ser apenas um elemento identificador para se tornar o combustível de uma economia baseada na vigilância e na análise preditiva. Contudo, surge uma nova e sensível fronteira informacional: a coleta de dados emocionais.

O conceito de privacidade emocional ganha relevância à medida que algoritmos de inteligência artificial, fundamentados por técnicas de biometria comportamental e análise de sentimento, passam a ser capazes de decodificar estados de ânimo, reações psicológicas e traços de personalidade dos usuários. Como observa Bruno Bioni (2019), a proteção de dados na "sociedade do controle" não visa apenas resguardar o segredo, mas garantir que o indivíduo não seja reduzido a um objeto de processamento informacional, preservando sua liberdade de escolha.

A questão principal deste estudo consiste no modo como é realizado o tratamento e exploração econômica dos dados sensíveis dos titulares e a proteção jurídica conferida a estes pela Lei nº 13.709, de 14 de agosto de 2018 (LGPD); assim como outras legislações vigentes que tratam do tema, como o Código de Defesa do Consumidor, o Código Civil e o Marco Civil da Internet. Embora a legislação brasileira tenha avançado ao estabelecer os princípios da finalidade (art. 7º), da necessidade (art. 7º), da transparência (art. 6º, IV), trazidos pela LGPD; que por si comunicam com o conceito de autodeterminação informativa — amplamente defendido por Danilo Doneda (2019) —, a opacidade dos termos de uso e a complexidade técnica dos sistemas de mineração de dados criam uma assimetria de poder que pode viciar o consentimento do titular.

Questiona-se, portanto: Quais são os limites jurídicos da coleta e do tratamento de dados de cunho emocional por plataformas digitais sob a ótica da legislação vigente, e em que medida a arquitetura de escolha dessas plataformas compromete a autodeterminação informativa e o livre desenvolvimento da personalidade do titular?

Para responder a tais inquietações, o presente trabalho objetiva analisar o impacto da coleta de dados sensíveis dos usuários no ordenamento jurídico brasileiro e como o tratamento destes dados afeta sua esfera íntima. Inicialmente, será abordada a evolução do direito à privacidade até a consolidação da proteção de dados pessoais. No segundo capítulo, o foco

recairá sobre as especificidades dos dados emocionais e os mecanismos de coleta das plataformas digitais. Por fim, serão discutidos os limites éticos e legais, bem como o papel das instituições reguladoras na proteção da privacidade emocional.

Para viabilizar a execução do desenho capitular proposto, a pesquisa adota uma abordagem qualitativa de natureza teórico-dogmática e caráter exploratório, utilizando o método dedutivo. O procedimento metodológico ancora-se na pesquisa bibliográfica e documental, realizada por meio do exame da legislação nacional — como a Lei Geral de Proteção de Dados de 2018, O Código Civil de 2002 e o Código de Defesa do Consumidor de 1990 —, de diretrizes de órgãos reguladores como a Autoridade Nacional de Proteção de Dados (ANPD), bem como a consulta à doutrina especializada e os artigos publicados sobre o tema. Dessa forma, busca-se confrontar a arquitetura de escolha das plataformas digitais com os parâmetros normativos vigentes, fundamentando as respostas ao problema proposto.

CAPÍTULO 1 - DELIMITAÇÕES CONCEITUAIS E EVOLUÇÃO JURÍDICA

Compreender os desafios que o tratamento de dados emocionais impõe ao ordenamento jurídico contemporâneo exige, antes de qualquer coisa, percorrer a genealogia do próprio conceito de privacidade. Esse percurso não é um exercício meramente histórico: é uma necessidade metodológica. A tentação de aplicar instrumentos clássicos a fenômenos radicalmente novos sem revisitar seus fundamentos produz respostas inadequadas — e é precisamente essa inadequação que explica por que o debate sobre a proteção de dados emocionais ainda carece de respostas jurídicas à altura de sua complexidade. Para que a autodeterminação informativa seja capaz de tutelar a subjetividade do titular frente à exploração algorítmica, é preciso primeiro entender de onde esse conceito veio, que problema veio resolver e em que medida os quadros normativos que o operacionalizam estão à altura do desafio contemporâneo.

Este capítulo percorre esse trajeto em três movimentos. O primeiro examina a formulação clássica do direito à privacidade como direito de ser deixado só, demonstrando que, desde sua origem, a proteção da esfera emocional já estava no horizonte da tutela jurídica, ainda que os instrumentos disponíveis fossem insuficientes para alcançá-la plenamente. O segundo analisa o surgimento da autodeterminação informativa como paradigma superador do isolamento estático, a partir do julgamento do Recenseamento de 1983 pelo Tribunal Constitucional Federal Alemão, e os reflexos desse novo paradigma na evolução legislativa da proteção de dados. O terceiro examina como esse fundamento dogmático se concretiza na arquitetura normativa da legislação brasileira, identificando as categorias jurídicas que embasarão a análise dos dados emocionais nos capítulos seguintes — e os limites que o próprio sistema ainda não superou.

1.1 O CONCEITO CLÁSSICO DE PRIVACIDADE E O *RIGHT TO BE LET ALONE*

Historicamente, a proteção à esfera íntima do indivíduo já transcendia a mera propriedade física, encontrando salvaguardas desde o Direito Romano, havendo alterações substanciais ao longo do tempo em relação à natureza das ameaças a esse espaço reservado. Nesse sentido, compreende-se que o debate jurídico moderno sobre a privacidade no mundo ocidental encontra um marco de reconfiguração no célebre artigo "The Right to Privacy", publicado em 1890 por Samuel Warren e Louis Brandeis. No contexto em que as fotografias instantâneas e o avanço do empreendimento jornalístico passaram a intervir nos ambientes cotidianos, os autores inovaram ao deslocar o foco da tutela jurídica para a proteção contra invasões imateriais, especificamente contra a divulgação não autorizada de fatos da vida privada.

Com a evolução dos direitos protegidos na esfera inteligível, nasceu a proteção da propriedade intelectual, relativa à inviolabilidade da personalidade, abrangida pelas músicas e mais diversas obras e criações artísticas, mas esta não era suficiente para resguardar todo o âmbito da vida privada, visto que há uma pluralidade de expressões que não se entendem como necessariamente artísticas ou intelectuais, mas que merecem resguardo da publicidade, pois afetam o indivíduo profundamente em aspectos relevantes da sua intimidade e tomada de decisões. Considerando esse raciocínio, compreende-se:

Semelhante proteção é conferida às emoções e sensações expressas em uma composição musical ou em outra obra de arte como em uma composição literária; e as palavras ditas, uma pantomima representada, uma sonata executada não têm menos direito à proteção do que se cada uma delas tivesse sido reduzida à escrita. A circunstância de que um pensamento ou emoção tenha sido registrado de forma permanente torna sua identificação mais fácil e, portanto, pode ser importante do ponto de vista probatório, porém, não tem importância como questão de direito substantivo. Se, então, as decisões indicam um direito geral à privacidade de pensamentos, emoções e sensações, estes devem receber a mesma proteção, seja expressa por escrito, seja na conduta, na conversa, nas atitudes ou na expressão facial (Brandeis; Warren, 2024, p. 405).

Diante disso, portanto, forma-se o pensamento de que a proteção jurídica não deve ser concedida apenas aos produtos conscientes do trabalho artístico e documental, mas também à solidão e privacidade do indivíduo, que devem ser considerados aspectos essenciais para a vida

digna humana em meio à era da informação. Essa transição conceitual alinha-se ao entendimento de Doneda (2006), citado por Cancelier (2016), para quem a desvinculação do *right to privacy* do direito de propriedade foi um marco fundamental, reposicionando o direito à privacidade na esfera mais íntima e intrínseca do indivíduo. Mesmo que o compartilhamento das informações captadas seja considerado "trivial", entende-se que "a trivialidade destrói ao mesmo tempo a robustez do pensamento e a delicadeza do sentimento" (Brandeis; Warren, 2024, p. 395).

Nessa longa evolução, cabe compreender que os direitos da personalidade — dos quais a privacidade é emanção direta — não constituem um catálogo estático de prerrogativas, mas uma cláusula aberta fundada na cláusula geral de tutela da dignidade da pessoa humana. Como bem articulam Dias e Melo (2023), a personalidade jurídica contemporânea é categoria essencialmente relacionada à promoção da dignidade do ser humano singular e concretamente considerado, razão pela qual os direitos dela derivados devem ser compreendidos como projeções físicas ou psíquicas da pessoa — não objetos dela —, o que afasta a confusão entre sujeito e objeto que historicamente dificultou sua tutela. Nesse sentido, compreende-se que emoções, como manifestações da psique e da subjetividade do indivíduo, integram o núcleo mais sensível desses direitos.

O *right to be let alone*, surgido dessa linha de pensamento, é melhor definido e delimitado na obra *Da privacidade à proteção de dados pessoais*, de Danilo Doneda (2006), onde se discute que, apesar de o centenário diagnóstico realizado pelos advogados de Boston ser valioso, ele deixou um problema fundamental: atualmente, a privacidade conceitua-se como muito mais do que apenas o isolamento do indivíduo em relação à sociedade, mas como algo muito mais complexo diante das atuais plataformas e ferramentas de captação de dados. No cenário contemporâneo, onde a relevância da informação é proporcional à evolução tecnológica, nota-se uma mudança estrutural no modelo de relacionamento do indivíduo com a esfera privada. O paradigma clássico da privacidade, inicialmente marcado por um individualismo que buscava a ausência de comunicação com terceiros — a chamada *zero-relationship* — torna-se insuficiente para delimitar o direito à privacidade na sociedade da informação (Doneda, 2006).

Nessa conjuntura, em que a tecnologia converte a informação em uma utilidade de custo reduzido e alto alcance, a tutela jurídica demanda a superação da visão limitada da privacidade, deslocando seu centro de gravidade do isolamento para o controle do fluxo informacional (Doneda, 2006). Assim, a proteção deixa de ser apenas um isolamento passivo para se tornar um pilar do livre desenvolvimento da personalidade humana. Conforme esclarece o autor:

Esta concepção foi o marco inicial; a temperá-la, posteriormente, temos a crescente consciência de que a privacidade é um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade (Doneda, 2006, p. 91).

Assim, o direito de ser deixado só transita de um mecanismo de reclusão para tornar-se condição imprescindível para que o sujeito preserve sua autonomia e individualidade, não sendo reduzido a mero objeto de processamento informacional e replicação comportamental. Nesse novo paradigma, como pontuam Dias e Melo (2023), a privacidade assume um caráter relacional — no qual se deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior —, afirmando-se em seu aspecto positivo de autodeterminação informativa, que assegura ao indivíduo o controle sobre suas informações e a construção da própria esfera privada.

1.2 A AUTODETERMINAÇÃO INFORMATIVA E A PROTEÇÃO DE DADOS PESSOAIS

A partir da evolução do conceito clássico de privacidade para a proteção dos direitos da personalidade como reflexo da dignidade da pessoa humana, como apontado por Dias e Melo (2023), a complexidade da sociedade da informação exigiu a criação de um novo paradigma: a autodeterminação informativa. Este conceito, mais alinhado com a necessidade de proteção da personalidade, traz a ideia do controle ativo do indivíduo sobre a circulação de suas informações. Essa mudança paradigmática encontra seu marco histórico na jurisprudência do Tribunal Constitucional Federal Alemão, especificamente no célebre julgamento do Recenseamento de 1983¹ (*Volkszählungsurteil*).

¹ O *Volkszählungsurteil* ("sentença do recenseamento") foi proferido pelo Tribunal Constitucional Federal Alemão em 15 de dezembro de 1983, ao julgar a constitucionalidade da Lei do Censo de 1982, que previa ampla coleta de dados dos cidadãos com possibilidade de transferência a outras autoridades federais. A Corte declarou parcialmente inconstitucional a lei, assentando que a dignidade da pessoa humana e o direito ao livre desenvolvimento da personalidade — arts. 1.1 e 2.1 da Lei Fundamental Alemã — fundam o direito fundamental à autodeterminação informativa.

Diante do armazenamento, processamento e transmissão de dados em escala imensuráveis, a formulação desse direito — cujas bases teóricas pioneiras remontam ao parecer de Steinmüller² e colaboradores em 1971 — buscou assegurar o livre desenvolvimento da personalidade frente a um cenário no qual o indivíduo perde progressivamente a capacidade de tomar decisões autônomas devido à opacidade e ubiquidade dos sistemas informatizados. A Corte Constitucional Alemã constatou que o direito ao livre desenvolvimento da personalidade, em conjunto com o princípio da dignidade humana, salvaguarda o direito fundamental à autodeterminação informativa, conceituado como o poder do indivíduo de determinar, em princípio, a revelação e a utilização de seus dados pessoais (Alemanha, 1983).

Na mesma sentença, foram fixados postulados fundamentais sobre os dados pessoais que persistem relevantes. O primeiro deles é o princípio da finalidade na coleta, de modo que dados recolhidos com um fim específico não podem ser utilizados para finalidade diversa. O segundo — e talvez o mais impactante para o debate contemporâneo — desmitificou a noção de que o tratamento de certos dados seria irrelevante para a tutela da privacidade: consolidou-se o entendimento de que um dado em si insignificante pode adquirir novo valor quando combinado com outros, de modo que não existem mais dados "insignificantes" no contexto do processamento eletrônico (Dias; Melo, 2023). Essa constatação é especialmente pertinente para a proteção da privacidade emocional, uma vez que interações aparentemente banais, como padrões de clique, tempo de visualização e expressões faciais captadas por câmeras, revelam, em seu conjunto, o estado afetivo do titular de forma precisa e potencialmente discriminatória.

Para neutralizar as ameaças advindas do processamento automatizado de dados, consolidou-se a tese de que todos os dados pessoais são tutelados pela autodeterminação informativa. Sob essa ótica, o controle sobre a extração, o manuseio e a difusão dessas informações pertencem, de forma privativa, ao próprio indivíduo, que assume o papel de gestor de sua própria identidade digital. Esse direito, como enfatizam Dias e Melo (2023), possui dupla dimensão: negativa, ao impor ao Estado e a terceiros a abstenção de tratar dados pessoais sem autorização, e positiva, ao impor ao Estado o dever de criar regras jurídicas reguladoras da utilização de informações pessoais, assegurando prestações normativas efetivas ao titular.

Em relação aos reflexos da autodeterminação informativa no âmbito legislativo, Bruno Bioni (2019), em sua obra *Proteção de dados pessoais: a função e os limites do consentimento*,

² STEINMÜLLER, Wilhelm et al. Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern. BT-Drucksache VI/3826, Anhang 1, 1971, p. 88-93. O ponto de partida deste parecer foi uma consulta do Ministério do Interior da Alemanha para delinear as bases da futura legislação de proteção de dados pessoais, propondo pioneiramente o modelo de controle procedimental do fluxo de informações.

entende que esse protagonismo do indivíduo em relação à utilização de seus dados pessoais origina uma "terceira geração" de leis de proteção de dados, onde a legislação não busca apenas proteger o dado, mas dar poder ao seu titular:

A amplitude desse papel de protagonismo do indivíduo na proteção dos dados pessoais é o divisor de águas para a terceira geração de leis. Nesse estágio, as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento. Alcançar-se-ia, assim, o êxtase da própria terminologia da "autodeterminação informacional", pois, com tal participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais (Bioni, 2019, p. 172).

Destaca-se ainda a ascensão de uma quarta geração de leis de proteção de dados, que surge para equilibrar o ônus decisório imposto ao titular pelo modelo de protagonismo absoluto da fase anterior (Bioni, 2019). Se a terceira geração atingiu o "êxtase" da autodeterminação ao centralizar tudo no consentimento, a quarta geração reconhece que essa sobrecarga informacional pode tornar a proteção ineficaz. Nesse estágio, o ordenamento jurídico passa a atuar de forma mais institucional e protetiva, focando em três pilares: a implementação de autoridades independentes — como a Autoridade Nacional de Proteção de Dados (ANPD) —, responsáveis por zelar, implementar e fiscalizar o cumprimento da norma; a relativização da centralidade do consentimento, ao admitir outras bases legais que oferecem proteção ao titular independentemente de sua manifestação de vontade; e a qualificação do consentimento, exigindo que este seja livre, informado, específico e inequívoco.

Essa relativização da centralidade do consentimento encontra fundamento positivo no próprio texto da LGPD, cujo art. 7º elenca dez hipóteses legais autônomas e não hierarquizadas que autorizam o tratamento de dados pessoais, dispensando, em cada uma delas, a manifestação de vontade do titular como requisito de licitude. Ao lado do consentimento (inciso I), a lei admite o tratamento fundado no cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), na execução de políticas públicas (inciso III), na realização de estudos por órgão de pesquisa (inciso IV), na execução de contrato do qual o titular seja parte (inciso V), no exercício regular de direitos em processo judicial, administrativo ou arbitral (inciso VI), na proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII), na tutela da

saúde (inciso VIII), no legítimo interesse do controlador ou de terceiro (inciso IX) e na proteção do crédito (inciso X). Essa pluralidade revela que o consentimento, embora historicamente erigido à condição de fundamento por excelência da autodeterminação informativa, não é pressuposto indispensável de toda e qualquer operação de tratamento. No campo dos dados emocionais, contudo, essa pluralidade impõe cautela redobrada: a elasticidade de bases como o legítimo interesse (art. 7º, IX) não pode servir de válvula de escape para o controlador contornar as garantias reforçadas exigidas pelo art. 11 da LGPD para dados sensíveis, cuja hipótese aplicável restringe-se, em regra, ao consentimento específico e destacado ou às hipóteses taxativas do parágrafo único do mesmo dispositivo — excluída, portanto, a invocação genérica do legítimo interesse para justificar a captura de estados emocionais.

É precisamente nesse ponto que a análise se conecta às advertências formuladas por Fernando Rodrigues Martins (2024) a respeito das lacunas éticas do sistema jurídico digital. Para o autor, o ordenamento contemporâneo depara-se com uma tripla perplexidade: a hipercomplexidade de suas fontes, a anomia em setores tecnologicamente avançados e a obsolescência normativa diante da velocidade das transformações digitais. No campo da privacidade emocional, esse quadro é particularmente agudo, pois a ausência de regulamentação específica para os chamados neurodireitos — como o direito à privacidade mental, à identidade e à liberdade de pensamento — abre lacunas que o sistema vigente ainda não consegue fechar por completo. Embora os instrumentos já existentes ofereçam uma base normativa relevante, a efetividade da proteção depende de uma atuação institucional ativa que preencha esses vazios antes que se tornem mecanismos estruturais de exclusão.

Dessa forma, apesar da consolidação da autodeterminação informativa como pilar da proteção de dados, a vulnerabilidade do indivíduo perante o processamento massivo de informações persiste. O equilíbrio desse cenário não se alcança apenas com a atribuição de titularidade, mas exige um auxílio estatal e normativo ativo que assegure a eficácia desse controle. Sem esse suporte institucional, o domínio sobre o fluxo informacional corre o risco de ser uma faculdade meramente simbólica. É apenas com a efetivação desses mecanismos de controle que se preserva a dignidade humana e o livre desenvolvimento da personalidade frente aos desafios impostos pela opacidade do cenário digital contemporâneo.

1.3 A AUTODETERMINAÇÃO INFORMATIVA E OS SISTEMAS NORMATIVOS DE PROTEÇÃO

A trajetória percorrida nos subcapítulos anteriores demonstrou que a privacidade evoluiu de um direito de isolamento estático para um direito de controle ativo sobre o fluxo informacional — e que essa transformação não ocorreu no vácuo, mas respondeu à progressiva incapacidade dos instrumentos clássicos de tutelar a subjetividade do indivíduo frente às novas formas de intrusão na esfera da personalidade. Esse deslocamento conceitual exige, agora, identificar como o ordenamento jurídico brasileiro internalizou esse paradigma e de que modo os diferentes diplomas normativos se articulam para conferir proteção efetiva à autodeterminação informativa — inclusive em sua dimensão mais sensível, que é a dos dados de cunho emocional.

A resposta do ordenamento brasileiro a esse desafio não se construiu por meio de um instrumento único, mas pela sedimentação progressiva de um diálogo integrado de fontes normativas. O Código Civil de 2002 estabeleceu, em seu art. 21, a inviolabilidade da vida privada como direito da personalidade oponível a todos, fixando a cláusula geral de tutela da pessoa humana que ancora dogmaticamente a proteção dos dados pessoais no direito privado. O Código de Defesa do Consumidor, embora anterior à era da proteção de dados em sentido estrito, consagrou princípios que se revelaram estruturantes para esse debate: o reconhecimento da vulnerabilidade do consumidor (art. 4º, I), o direito à informação adequada e clara (art. 6º, III) e a responsabilidade objetiva do fornecedor pelo defeito do serviço (art. 14). Esses dispositivos, interpretados à luz da dignidade humana e da boa-fé objetiva, projetam-se naturalmente sobre as relações entre plataformas digitais e titulares de dados, cujo desequilíbrio estrutural é, no mínimo, tão acentuado quanto o da relação de consumo tradicional.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) veio densificar esse arcabouço, ao eleger, em seu art. 2º, a privacidade, a autodeterminação informativa, a dignidade e o livre desenvolvimento da personalidade como fundamentos expressos da proteção de dados — não criando um regime paralelo ao Código Civil e ao Código de Defesa do Consumidor, mas estabelecendo um eixo valorativo comum que demanda a interpretação coordenada e harmônica dessas fontes. Ainda que esse conjunto normativo não configure, tecnicamente, um microsistema completo e autossuficiente para a proteção de dados no ambiente digital —

lacuna que é ela mesma parte do problema regulatório que este trabalho identifica —, a sua articulação hermenêutica oferece base suficiente para a tutela da autodeterminação informativa, inclusive em sua dimensão emocional. Portanto, nesse contexto, entende-se que foi estabelecido um eixo valorativo comum que demanda a interpretação integrada e harmônica dessas fontes — o que a doutrina tem designado como diálogo das fontes (Martins, 2024).

Nesse diálogo, a distinção entre dado pessoal e dado sensível, estabelecida no art. 5º da LGPD, ganha especial relevo. O dado pessoal (inciso I) abrange toda informação que identifique ou torne identificável o titular, categoria que engloba os rastros digitais e perfis comportamentais produzidos nas plataformas. O dado sensível (inciso II) recebe proteção qualificada precisamente porque sua exposição potencializa riscos de discriminação e de lesão ao núcleo mais íntimo da personalidade — o que justifica, no plano normativo, a imposição de bases legais mais restritas para o seu tratamento. Embora as emoções não constem literalmente desse rol, a interpretação sistemática da norma, à luz dos critérios do potencial discriminatório e da natureza biométrica e comportamental dos mecanismos de captura afetiva, permite enquadrá-las nessa categoria protetiva mais rigorosa (Bioni, 2019).

A articulação desses sistemas normativos implica, ainda, consequências relevantes para a responsabilidade civil. O controlador que estrutura sua atividade sobre o tratamento de dados emocionais sem observância dos princípios da finalidade, da necessidade e da transparência — previstos no art. 6º da LGPD — não apenas descumpre obrigação legal específica, mas viola simultaneamente a cláusula geral de tutela da personalidade do Código Civil e o dever qualificado de informação do CDC. Essa sobreposição normativa não gera conflito, mas amplia a proteção do titular: o dano decorrente do tratamento irregular de dados emocionais é passível de reparação tanto pela via da responsabilidade objetiva do fornecedor de serviços digitais, nos termos do art. 14 do CDC, quanto pelo regime específico do art. 42 da LGPD, que igualmente prescinde da demonstração de culpa. A análise aprofundada dessas hipóteses de responsabilização e dos desafios que o dano emocional impõe à sua configuração constituirá objeto de análise posterior no trabalho.

Por ora, o que importa assentar é que a autodeterminação informativa, tal como se sedimentou no ordenamento brasileiro, não é um princípio isolado da LGPD: é o fio condutor que atravessa o Código Civil, o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados, impondo a todos os agentes de tratamento o dever de respeitar o indivíduo como sujeito de sua própria informação — e não como objeto de exploração algorítmica. É sobre essa base

normativa integrada que os capítulos seguintes analisarão os mecanismos de coleta de dados emocionais e os limites jurídicos que o ordenamento opõe à sua mercantilização.

CAPÍTULO 2 – A PRIVACIDADE EMOCIONAL E A COLETA DE DADOS SENSÍVEIS

Este segundo capítulo tem como objetivo aprofundar o debate sobre a Privacidade Emocional, investigando como o tratamento de estados de ânimo e reações psíquicas se insere no ordenamento jurídico brasileiro. Após a fundamentação da proteção de dados como um novo direito da personalidade, será analisado agora a transição da vigilância de dados objetivos para a decodificação da subjetividade humana, cenário em que a instrumentalização informacional da essência do indivíduo passa a ser o motor da economia digital.

A jornada desta seção percorre desde a complexa definição jurídica dos dados emocionais — frequentemente situados em uma zona cinzenta entre o dado comum e o sensível — até a análise dos mecanismos técnicos de captura, como a biometria comportamental e os algoritmos de análise de sentimento. Essa base técnica e teórica é indispensável para a compreensão, ao final deste capítulo, como a "arquitetura de escolha" das plataformas digitais impacta a autonomia do usuário e provoca uma crise no paradigma clássico do consentimento.

2.1 DEFINIÇÃO DE DADOS EMOCIONAIS COMO DADOS SENSÍVEIS

Segundo a perspectiva de Mikhail Cancelier (2016), a privacidade deixou de ser um bem resguardado pelo isolamento para se tornar algo de que o sujeito busca, muitas vezes, evadir-se. Nesse contexto, a existência social nas plataformas digitais passa a praticamente depender da publicização da intimidade, onde as emoções não são apenas sentidas, mas convertidas em ativos de visibilidade e pertencimento no cenário contemporâneo. O autor argumenta que essa necessidade de ser "visto" e "notado" cria um ambiente onde a proteção da esfera emocional é fragilizada pela própria conduta do titular, que entrega sua subjetividade ao fluxo informacional em troca de validação social, ele sintetiza:

O que se percebe é que, com a popularização da internet, para além da intensificação da invasão da privacidade, a população passou a exercer um movimento

de evasão da privacidade, enaltecendo a exposição deliberada de suas informações privadas. A precisão de Bauman (2014, p. 47) é notável: "o medo da exposição foi abafado pela alegria de ser notado".

Se, por um lado, a evasão da privacidade descrita por Cancelier (2016) demonstra uma entrega voluntária de dados em busca de validação social, por outro, o ecossistema digital se aproveita dessa abertura para operar uma captura invisível. É nesse cenário de assimetria que se sustenta a tese de Bruno Bioni (2019) sobre os "dados triviais sensibilizados": o risco não reside apenas naquilo que o titular expõe conscientemente, mas em como interações aparentemente inofensivas — como curtidas, tempos de visualização ou padrões de interação — são refinadas e cruzadas de forma oculta por algoritmos de análise preditiva (ex.: *Big Data*)¹ para revelar traços íntimos da personalidade e prever comportamentos, transmutando-se em vetores de vulnerabilidade capazes de expor a essência subjetiva do indivíduo ao controle e influência de terceiros. Com base nesse raciocínio, o autor atesta:

Por tal razão, a proteção dos dados pessoais perpassa a própria tutela do princípio da isonomia, na medida em que é um instrumento de contenção às práticas discriminatórias. Exatamente por esse motivo leis de proteção de dados pessoais, incluindo a brasileira, dedicam um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias. (Bioni, 2019, p. 119)

Nesse contexto, surge o desafio de enquadramento legal: embora o artigo 5º, inciso II, da Lei Geral de Proteção de Dados (LGPD) não mencione explicitamente as "emoções" dentre a classificação de dados sensíveis, entende-se que a interpretação sistemática da norma permite essa classificação.

Fundamentando-se na doutrina de Bioni (2019), a tipificação dos dados sensíveis deve ser compreendida sob a ótica do potencial discriminatório: não se trata de verificar se o dado se encaixa formalmente em uma das categorias enumeradas no art. 5º, inciso II, da LGPD, mas de avaliar se o seu tratamento é capaz de expor o titular a práticas discriminatórias ou de instrumentalizar sua subjetividade contra seus próprios interesses. Sob esse critério interpretativo, os dados emocionais revelam propensões psicológicas, estados de ânimo e aspectos da intimidade que, quando processados por sistemas de perfilamento preditivo, conferem ao controlador um poder de influência sobre o titular que justifica o regime protetivo mais rigoroso da norma. Ademais, quando a captura emocional ocorre por meio de

reconhecimento facial ou análise da voz, o dado enquadra-se diretamente na categoria de biometria, expressamente protegida pela lei.

Essa moldura conceitual encontra ressonância na própria trajetória normativa da proteção de dados no Brasil. Conforme demonstram Marques e Martins (2024), foi o Código de Defesa do Consumidor — e não a legislação especificamente voltada à privacidade — que introduziu pioneiramente os "dados pessoais" no sistema jurídico interno, ao disciplinar no art. 43 a atividade dos bancos de dados de consumidores e exigir, entre outros deveres, a acessibilidade, a objetividade e a veracidade das informações arquivadas. Os autores destacam que a causa subjacente dessa inserção pioneira sempre foi a tutela de interesses fundamentais associados à privacidade, entre os quais se incluem informações referentes à vida íntima e ao modo de ser do indivíduo. Esse percurso normativo, que parte do CDC e culmina no reconhecimento da proteção de dados como direito fundamental autônomo pela Emenda Constitucional 115/2022, demonstra que a tutela da esfera mais íntima da pessoa — incluindo, por extensão lógica, os estados afetivos e emocionais — não é uma novidade exógena ao sistema brasileiro, mas a continuidade de uma trajetória protetiva já inaugurada há mais de três décadas.

Portanto, a distinção dos dados emocionais como sensíveis justifica-se pelo fato de que eles tocam o núcleo da autodeterminação informativa. Conforme indica a perspectiva de Bioni (2019), apropriada por Bohrer (2019), é por meio do *online profiling*³ que se opera a sensibilização definitiva de registros inicialmente comuns. O tratamento preditivo das reações afetivas transmuta interações banais em um poderoso instrumento de classificação da personalidade, o que justifica a imposição do regime protetivo mais rigoroso da LGPD como salvaguarda necessária para frear a erosão da esfera íntima do titular.

³ O online profiling consiste no processo de coleta e tratamento automatizado de dados pessoais com o objetivo de avaliar, analisar ou prever aspectos específicos da personalidade, comportamento, interesses e estados emocionais de um indivíduo. Essa técnica permite a criação de perfis comportamentais detalhados que servem de base para a tomada de decisões automatizadas e a personalização de conteúdos no ambiente digital (BOHRER, 2019; BIONI, 2019).

2.2 ALGORITMOS DE ANÁLISE DE SENTIMENTO E BIOMETRIA COMPORTAMENTAL

A tecnologia por trás dessa exploração comercial das emoções não é recente, remontando à própria cunhagem do termo *affective computing* por Rosalind Picard (1995), pesquisadora do MIT Media Laboratory, que definiu o campo como o conjunto de técnicas computacionais que se relacionam, decorrem ou influenciam as emoções humanas. Já nessa formulação seminal, a autora demonstrou, com apoio em estudos neurológicos sobre pacientes com lesões no lobo frontal, que a emoção não constitui elemento marginal ou irracional a ser suprimido pelos sistemas computacionais, mas componente estrutural da própria capacidade humana de decisão — o que justificou, do ponto de vista técnico, o interesse crescente da indústria em modelar e antecipar estados afetivos como via de otimização preditiva do comportamento do usuário. Picard (1995) descreve, ainda, um conjunto de canais fisiológicos passíveis de captura para a inferência do chamado "estado sêntico" do indivíduo — expressão facial, inflexão vocal, condutância da pele, frequência cardíaca, pressão digital e padrões respiratórios —, muitos dos quais operam de forma involuntária e, portanto, inacessível ao controle consciente do próprio titular. É justamente essa captura de sinais fisiológicos involuntários, sistematizada já nos primórdios da computação afetiva, que hoje sustenta tecnicamente os algoritmos de análise de sentimento e biometria comportamental empregados pelas plataformas digitais, conferindo densidade histórica e científica à premissa de que o monitoramento emocional alcança dimensões da personalidade que escapam à própria vontade consciente do titular.

A evolução das estratégias de monitoramento e processamento de dados no ambiente digital marca o ápice da exploração de dados: a interioridade do indivíduo. Conforme sustenta Bioni (2019), o modelo de publicidade contemporâneo superou a mera análise de dados externos como geolocalização ou de histórico de compras para inaugurar a era da publicidade baseada em emoções.

Nesse cenário, o usuário é inserido no conceito de "consumidor de vidro", uma metáfora para a transparência absoluta da psique frente aos sensores e algoritmos (Bioni, 2019). O autor esclarece que as plataformas utilizam tecnologias de reconhecimento facial, análise de tom de voz e sensores de movimento para mapear reações afetivas em tempo real, permitindo que o controlador identifique não apenas o que o titular deseja, mas em qual estado emocional ele se

encontra no exato momento da oferta, explorando vulnerabilidades psicológicas para otimizar o engajamento e a conversão comercial, ele disserta:

É uma realidade, portanto, a estruturação de bases de dados de emoções, a fim de personalizar ainda mais a ação publicitária. Há, por isso, uma vigilância imperativa das pessoas, em especial do potencial consumidor, o que varia desde os seus hábitos de navegação e comportamento na Internet às suas próprias emoções, tornando-o, totalmente, transparente. (Bioni, 2019, p. 46-47).

Essa captura incessante da subjetividade encontra seu suporte operacional no *online profiling*, que transcende a simples organização de informações para se tornar uma engenharia de predição comportamental. Segundo Bohrer (2019), o *profiling* resulta das técnicas de *data mining*⁴ e consiste no processo pelo qual o tratamento de dados, mediante métodos estatísticos e tecnologia de inteligência artificial, dá origem à elaboração de um perfil virtual de um indivíduo pautado em comportamentos, hábitos e padrões tidos como confiáveis para a tomada de decisões a respeito daqueles que são avaliados.

A profundidade dessa técnica reside em sua natureza prospectiva: não se busca compreender o passado do indivíduo, mas antecipar suas condutas futuras por inferências algorítmicas, o que pode isolar o usuário em bolhas informacionais e abrir espaço a práticas discriminatórias, na medida em que o perfil construído categoriza o indivíduo em rótulos de risco ou interesse sem o seu conhecimento (Bohrer, 2019).

Esse processo de perfilamento materializa-se tecnicamente em algumas etapas concretas e sucessivas. Conforme sistematiza Zanatta (2019), a perfilização compreende, pelo menos, as fases de registro dos dados, agregação e monitoramento, identificação de padrões, interpretação de resultados, novo monitoramento para checagem e, por fim, aplicação dos perfis construídos. É justamente nessa etapa final de aplicação que a vulnerabilidade do titular se manifesta de forma mais aguda: o perfil inferido a partir do comportamento passado não é apresentado ao titular para validação, mas utilizado diretamente para limitar e direcionar o rol de escolhas futuras daquela pessoa (Doreto; Borges; Ferreira, 2026).

Por fim, a integração desses mecanismos de captura e perfilamento consolida o paradigma da vigilância líquida, conforme analisado por Cancelier (2016) sob a ótica de

⁴ O *data mining* consiste no processo estatístico e automatizado pelo qual algoritmos exploram uma base de dados bruta com o objetivo de descobrir padrões ocultos e extrair conhecimento aplicado para subsidiar decisões prospectivas (BOHRER, 2019, p. 76).

Zygmunt Bauman. Diferentemente do panóptico clássico, onde a vigilância era fixa e punitiva, a modalidade líquida é caracterizada por sua fluidez e ubiquidade, infiltrando-se nas esferas mais íntimas do cotidiano sem encontrar resistências geográficas ou temporais.

Nessa dinâmica, o monitoramento das emoções deixa de ser apenas uma intrusão externa forçada pelas plataformas, tornando-se uma simbiose entre o desejo do usuário de ser notado e o interesse das plataformas em processar cada reação afetiva. O resultado é a consolidação de uma sociedade de controle onde a privacidade emocional e a proteção de direitos fundamentais se encontram fragilizadas não apenas pela técnica, mas pela própria reconfiguração cultural do "direito de estar só" (Cancelier, 2016).

2.3 VULNERABILIDADE DIGITAL E ALGORÍTMICA: A EXPLORAÇÃO DO TITULAR PELOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Os mecanismos de coleta examinados na seção anterior não operam sobre um titular abstrato e equidistante. Sua eficácia depende de uma condição prévia do sujeito sobre o qual incidem: a vulnerabilidade. Importa, portanto, investigar essa condição em suas múltiplas camadas, demonstrando que a exploração de dados emocionais por sistemas de inteligência artificial não é um desvio pontual de conduta de certos agentes econômicos, mas o produto esperado de uma arquitetura informacional estruturalmente desequilibrada.

A primeira camada dessa condição estrutural é a que Madalena (2025) denomina vulnerabilidade digital — fenômeno que, segundo o autor, decorre da própria forma como a sociedade contemporânea organiza suas instituições sociais, tornando-as dependentes de estruturas digitais para o acesso a serviços, o consumo e a convivência. O autor sustenta que o uso de dados para explorar predisposições cognitivas e emocionais inaugura um ambiente em que qualquer consumidor pode ser afetado, independentemente de seu pertencimento a determinado grupo ou de dispor de alguma condição pessoal que agrave sua vulnerabilidade. Diferentemente das concepções tradicionais do direito do consumidor, que diferenciavam o "consumidor médio" do "consumidor vulnerável", a lógica digital dissolve essa fronteira: todos se tornam suscetíveis ao poder das plataformas e dos sistemas de recomendação baseados em dados. Por essa razão, o autor defende a superação dos modelos de vulnerabilidade fundados em condição individual ou em grupos específicos, propondo o reconhecimento de um *standard*

geral de vulnerabilidade que decorre da própria arquitetura digital à qual todos os indivíduos estão submetidos (Madalena, 2025).

Madalena (2025) acrescenta que essa universalização da vulnerabilidade decorre, em grande medida, da opacidade algorítmica que caracteriza os sistemas digitais: enquanto as plataformas dominam integralmente os mecanismos de coleta, processamento e interpretação dos dados, os usuários permanecem na condição de destinatários passivos, incapazes de questionar ou prever de que modo suas informações estão sendo utilizadas — circunstância que compromete diretamente a autodeterminação informativa do titular. A vulnerabilidade digital, nesse sentido, não constitui um atributo do sujeito, mas uma propriedade emergente da própria relação entre indivíduo e sistema, o que justifica seu reconhecimento como categoria jurídica autônoma, distinta da vulnerabilidade do consumidor já consagrada pelo art. 4º, I, do Código de Defesa do Consumidor.

Sobre esse piso estrutural, determinados grupos enfrentam uma camada adicional de exposição, qualificada por características pessoais que intensificam o risco de captura da vontade. É o que ocorre com crianças e adolescentes diante dos sistemas de inteligência artificial voltados à publicidade e ao engajamento digital. Holanda e Costa (2026) demonstram que o neurodesenvolvimento infantil torna esse público especialmente suscetível a estímulos persuasivos, uma vez que o córtex pré-frontal — uma das regiões mais complexas do cérebro humano, responsável por funções executivas como o raciocínio, a organização de pensamentos e a tomada de decisões informadas — ainda se encontra em desenvolvimento nessa fase da vida, comprometendo a plena capacidade de avaliação e controle dos impulsos. Segundo os autores, a dependência humana em relação às mídias sociais está relacionada à liberação de dopamina no cérebro, o que estimula um ciclo vicioso de experiências imediatas de prazer e bem-estar, circunstância deliberadamente potencializada por técnicas persuasivas como a gamificação e o *scroll* infinito⁵, que exploram diretamente essas fragilidades neurológicas (Holanda; Costa, 2026).

Holanda e Costa (2026) sustentam que essa imaturidade neurocognitiva não é apenas uma constatação da neurociência do desenvolvimento, mas encontra correspondência jurídica

⁵ *scroll* infinito é uma técnica de *design* que recarrega o conteúdo de forma contínua à medida que o usuário rola a página, dispensando a necessidade de cliques para mudança de tela e eliminando a possibilidade de se deparar com o esgotamento do conteúdo. O próprio criador da ferramenta, Aza Raskin, denominou a técnica como "cocaína comportamental", em razão do seu alto potencial viciante. A ferramenta funciona como um prazer efêmero que não proporciona verdadeira sensação de satisfação ou saciedade: o cérebro é condicionado a buscar o próximo estímulo, criando um ciclo de insatisfação permanente. Em crianças e adolescentes, cujas funções cognitivas relacionadas ao autocontrole e ao julgamento crítico ainda estão em desenvolvimento, essa técnica aumenta significativamente a exposição a conteúdos comerciais direcionados por algoritmos, intensificando os riscos associados ao consumo e à manipulação digital (HOLANDA; COSTA, 2026).

direta no art. 37, § 2º, do Código de Defesa do Consumidor, que reconhece como abusiva a publicidade que se aproveite da deficiência de julgamento e da inexperiência da criança. Os autores classificam crianças e adolescentes, em razão dessas peculiaridades, como pessoas hipervulneráveis no mercado de consumo digital — categoria que, conforme será examinado adiante, qualifica a vulnerabilidade comum sem, contudo, substituí-la ou afastá-la, somando-se a ela.

Sobre essas duas camadas — a universal e a qualificada — incide ainda uma terceira dimensão, específica da arquitetura técnica dos sistemas de inteligência artificial: a vulnerabilidade algorítmica propriamente dita. Doreto, Borges e Ferreira (2026) demonstram que a incorporação massiva de tecnologias digitais ao consumo produziu uma verdadeira mutação estrutural nas relações de mercado: o fornecedor deixou de ser um sujeito claramente identificável para operar como uma rede automatizada e desterritorializada, enquanto o consumidor passou a interagir com sistemas despersonalizados, muitas vezes sem sequer saber quem efetivamente controla os fluxos de informação que o atingem. Essa reconfiguração ampliou a assimetria informacional, que antes se restringia ao conhecimento sobre produtos e passou a envolver dados pessoais, comportamentos e vulnerabilidades cognitivas, intensificadas pela personalização algorítmica e por estratégias persuasivas que capturam atenção e antecipam decisões.

Os autores sistematizam essa transformação em três camadas interdependentes, que se sobrepõem e se reforçam mutuamente. A vulnerabilidade tecnológica representa o ponto de partida estrutural, decorrente do descompasso entre a sofisticação dos sistemas e a capacidade do consumidor de compreendê-los ou utilizá-los criticamente: mesmo quando o acesso aos dispositivos é possível, a ausência de literacia tecnológica impede que o titular compreenda os fluxos de dados, os protocolos de segurança ou as dinâmicas de vigilância embutidas em interfaces aparentemente neutras. A vulnerabilidade digital, por sua vez, desloca o foco da exclusão tecnológica para o próprio desenho estrutural das plataformas: interfaces persuasivas, curadorias algorítmicas e *nudges*⁶ condicionam escolhas, capturam atenção e reduzem a autonomia do usuário, em uma assimetria transversal típica do que a doutrina denomina capitalismo de vigilância. Por fim, a vulnerabilidade algorítmica aprofunda essa lógica ao

⁶ O termo *nudge* (literalmente, "empurrãozinho" ou indução sutil), oriundo da Economia Comportamental (THALER; SUNSTEIN, 2008), designa qualquer aspecto da "arquitetura de escolhas" que altera o comportamento das pessoas de forma previsível, sem proibir nenhuma opção ou alterar significativamente seus incentivos econômicos. No ambiente digital (*digital nudging*), a técnica é instrumentalizada por meio do desenho de interfaces e curadorias algorítmicas para explorar vieses cognitivos e conduzir sutilmente o usuário a comportamentos que favorecem a coleta de dados pessoais, mitigando sua autonomia (BIONI, 2019, Cap. IV, subitem 4.2.4).

transferir o próprio controle da experiência de consumo para sistemas automatizados de decisão: o consumidor passa a interagir com um ambiente que não apenas influencia suas escolhas, mas antecipa e remodela suas preferências com base em inferências probabilísticas, mascarando assimetrias sob a aparência de neutralidade técnica (Doreto; Borges; Ferreira, 2026).

Diante dessa tríplice vulnerabilidade, Doreto, Borges e Ferreira (2026) sustentam que a mera responsabilização *ex post* — isto é, a reparação do dano após sua ocorrência — revela-se insuficiente, impondo a necessidade de uma arquitetura de responsabilidade multifuncional, que os autores descrevem, com apoio em Nelson Rosenvald e José Luiz de Moura Faleiros Júnior, como a combinação entre *accountability* (governança, auditorias independentes, padrões técnicos e prestação de contas) e *answerability* (explicabilidade e vias céleres de contestação e revisão humana das decisões automatizadas). Segundo essa formulação, a tutela jurídica deve migrar da reparação isolada para um regime de governança responsiva, que reequilibre o poder informacional e trate dados e algoritmos como dever jurídico estruturante — e não como mera boa prática corporativa (Doreto; Borges; Ferreira, 2026).

É justamente nesse ponto que a vulnerabilidade algorítmica dialoga com a categoria da hipervulnerabilidade examinada anteriormente em relação a crianças e adolescentes. Doreto, Borges e Ferreira (2026) esclarecem, com apoio em Claudia Lima Marques, que a hipervulnerabilidade não constitui uma nova categoria autônoma, mas uma qualificação da vulnerabilidade já existente, que impõe ao intérprete o dever de calibrar a proteção segundo as condições concretas do sujeito — idade, deficiência, enfermidade, analfabetismo ou precariedade socioeconômica —, de modo a assegurar igualdade material de oportunidades e decisões efetivamente livres e informadas. É sobre essa categoria que se assentam os marcos regulatórios mais recentes em matéria de inteligência artificial: o art. 5º do *AI Act* europeu proíbe a colocação no mercado de sistemas de IA que explorem vulnerabilidades de pessoas ou grupos específicos em razão de idade, deficiência ou situação social ou econômica, quando tal exploração tenha por objetivo ou efeito distorcer materialmente o comportamento do indivíduo e causar dano significativo. No mesmo sentido, o art. 14 do Projeto de Lei 2.338/2023 qualifica como risco excessivo o emprego de técnicas subliminares para indução de comportamentos prejudiciais e a exploração de vulnerabilidades de grupos específicos para induzir comportamentos danosos (Doreto; Borges; Ferreira, 2026).

A leitura conjunta dessas três camadas — a vulnerabilidade digital universal identificada por Madalena (2025), a hipervulnerabilidade qualificada de crianças e adolescentes examinada por Holanda e Costa (2026), e a tríplice vulnerabilidade tecnológica, digital e algorítmica

sistematizada por Doreto, Borges e Ferreira (2026) — revela que a exploração de dados emocionais não constitui uma falha eventual do mercado digital, mas uma característica estrutural de seu próprio funcionamento. As plataformas não apenas se beneficiam da vulnerabilidade do titular: elas a produzem e a intensificam por meio do design dos sistemas que operam. Essa constatação possui consequência jurídica direta — se a vulnerabilidade é estrutural e não excepcional, os instrumentos de proteção também devem deixar de operar de forma pontual e reativa. É precisamente no espaço em que essa vulnerabilidade se converte em ato jurídico — o consentimento do titular para o tratamento de seus dados emocionais — que a fragilidade do sistema brasileiro se revela de forma mais evidente, tema que será examinado no subcapítulo seguinte.

2.4 A "ARQUITETURA DE ESCOLHA" E A CRISE DO CONSENTIMENTO NAS PLATAFORMAS DIGITAIS

Se os mecanismos de coleta e a vulnerabilidade estrutural analisados nas seções anteriores revelam a dimensão técnica da exploração emocional do usuário, entende-se que na dimensão jurídica encontra-se o paradoxo relevante da proteção de dados na contemporaneidade: o consentimento, como instrumento central eleito pelo ordenamento para legitimar o tratamento de dados, encontra-se estruturalmente comprometido pela própria dinâmica das plataformas que o deveria regular.

Para compreensão dessa crise, deve-se examinar o modo como as plataformas digitais arquitetam as escolhas de seus usuários. O conceito de "arquitetura de escolha", oriundo da economia comportamental, designa o conjunto de elementos que compõem o contexto em que uma decisão é tomada; ou seja, a forma como as opções são apresentadas e a ordem em que aparecem e os estímulos cognitivos que envolvem o ato de escolher. No ambiente digital, essa arquitetura é projetada para conduzir o usuário a comportamentos que justamente favorecem a coleta de dados pessoais, explorando a assimetria entre gratificações imediatas e prejuízos mediatos (Bioni, 2019).

Essa dinâmica é agravada de maneira singular quando o objeto do processamento são os dados emocionais: os sistemas de biometria comportamental e análise de sentimento permitem calibrar a própria interface em tempo real, apresentando solicitações de permissão nos momentos em que o usuário se encontra em estado de baixa resistência cognitiva —

ansiedade, tédio ou impulsividade — aumentando a probabilidade de aceitação. O consentimento colhido sob essa influência não é livre, pois ele é, antes, um ato condicionado pela exploração emocional do próprio titular. Sobre esse entendimento, argumenta-se:

O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócios da economia digital, do que como um meio eficiente para desempenhar a proteção dos dados pessoais. Ele tem sido encarado como uma verdadeira ficção legal deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática. Não seria mais do que uma mistificação, na medida em que não é confrontado com o anotado contexto socioeconômico que estrangula a prometida liberdade da autodeterminação informacional. (Bioni, 2019, p. 164)

O canal por excelência da operacionalização do consentimento nas plataformas digitais são as políticas de privacidade, e estas revelam-se igualmente problemáticas. Isto revela-se nos contratos de adesão predispostos unilateralmente pelo controlador, que conferem ao usuário apenas a escolha de aceitar ou abdicar do serviço completamente, o que elimina, na prática, qualquer capacidade de negociação do titular sobre seus dados (Bioni, 2019).

Essa fragilidade contratual é tecnicamente potencializada pelas práticas de design denominadas *dark patterns* — padrões obscuros de interface que induzem ou impedem escolhas contrárias ao interesse do usuário. Marques, Mendes e Bergstein (2023) demonstram que tais práticas podem ser descritas como interfaces utilizadas por empresas digitais para levar os consumidores a tomar decisões que não tomariam caso estivessem plenamente informados e capazes de avaliar alternativas. As autoras catalogam, entre os exemplos mais relevantes para o presente contexto, as assinaturas ocultas — em que o consumidor incorre em taxa recorrente sob o pretexto de período experimental gratuito —, a má direção, que utiliza o visual, a linguagem e a própria emoção para guiar o usuário em direção a uma escolha que interessa à plataforma, e as perguntas enganosas, nas quais o preenchimento de um formulário induz o consumidor a fornecer uma resposta diferente daquela que pretendia (Marques; Mendes; Bergstein, 2023).

Sob a ótica do direito brasileiro, Marques, Mendes e Bergstein (2023) sustentam que essas práticas podem ser enquadradas como abusivas nos termos do art. 39 do Código de Defesa do Consumidor, na medida em que se aproveitam da fraqueza ou da ignorância do consumidor para lhe impor produtos, serviços ou condições que ele não teria aceitado em circunstâncias de equilíbrio informacional.

Em todos esses casos, compreende-se que o resultado é um cenário onde o usuário é induzido a uma escolha que não reflete sua vontade autônoma, mas a vontade estrutural da plataforma manifestada por meio da interface. Essas práticas desnaturam por completo os requisitos do consentimento válido previstos no artigo 8º da Lei Geral de Proteção de Dados (LGPD), que exige seja ele livre, informado, específico e inequívoco (Bioni, 2019).

Nesse cenário, os efeitos do *online profiling* baseado em dados emocionais aprofundam, de forma qualificada, a vulnerabilidade do titular dentro da própria arquitetura de escolha projetada pelas interfaces. Quando o perfilamento comportamental passa a incorporar dados de natureza emocional, a identidade digital construída deixa de ser um agrupamento meramente estatístico de preferências de consumo para se converter em um indicador dinâmico do estado afetivo do usuário em cada momento de interação — sem que o titular tenha meios de antecipar as consequências dessa aplicação, o que compromete a própria base do consentimento informado (Bohrer, 2019).

Tampouco o aprimoramento legislativo em curso dissolve, por si só, essa crise estrutural. Marques e Martins (2024) observam que o mundo digital representa um desafio para o qual grande parte dos melhores instrumentos ainda reside nos lindes do direito do consumidor — sistema que, desde a edição do CDC, mostrou-se capaz de absorver a assimetria estrutural entre fornecedores e destinatários finais como pressuposto normativo de proteção, e não como acidente corrigível pontualmente. Os autores apontam que a aprovação do Projeto de Lei 3.514/2015, voltado à atualização do CDC para a disciplina do comércio eletrônico, é urgente precisamente porque reforça, como direito básico do consumidor, a privacidade e a segurança das informações e dos dados pessoais prestados ou coletados, além de prever expressamente, entre os objetivos da regulação do comércio eletrônico, a diminuição da assimetria de informações e a proteção da autodeterminação e da privacidade dos dados pessoais (Marques; Martins, 2024).

Portanto, a crise do consentimento não é uma falha acidental de implementação corrigível com termos de uso mais claros ou exigências formais adicionais. É uma crise estrutural, enraizada na assimetria fundamental entre o poder técnico, econômico e informacional das plataformas digitais e a vulnerabilidade — digital, hipervulnerável e algorítmica — do titular, conforme diagnostica Bioni (2019) ao caracterizar o consentimento como uma "ficção legal" que legitima modelos de negócios em lugar de desempenhar função genuinamente protetiva. A arquitetura da rede, enquanto não submetida a uma intervenção regulatória que a subordine aos fins da proteção de dados, tenderá a funcionar como instrumento de neutralização da autonomia do titular. Diante dessa constatação, a análise deve avançar para

o exame dos instrumentos jurídicos disponíveis no ordenamento brasileiro para enfrentar esse desequilíbrio, tarefa que constitui o objeto do capítulo seguinte.

CAPÍTULO 3 – LIMITES JURÍDICOS E A EFETIVIDADE DA PROTEÇÃO NO BRASIL

Este terceiro capítulo tem como objetivo examinar os instrumentos jurídicos disponíveis no ordenamento brasileiro para enfrentar os desequilíbrios identificados nos capítulos anteriores. Após fundamentada a proteção de dados emocionais como imperativo dogmático e demonstrado como a arquitetura das plataformas digitais compromete estruturalmente o consentimento do titular, cabe agora investigar se — e em que medida — o aparato normativo e institucional brasileiro é capaz de responder a esses desafios com efetividade.

A jornada desta seção percorre três eixos complementares. Primeiramente, será analisado o papel da Autoridade Nacional de Proteção de Dados (ANPD) como instância regulatória especializada, verificando sua capacidade de fiscalizar e orientar o uso de tecnologias de reconhecimento emocional frente à velocidade do desenvolvimento técnico. Em seguida, serão examinados os desafios impostos à responsabilidade civil quando o dano decorre do tratamento irregular de dados emocionais, cujas consequências frequentemente são invisíveis, difusas e de difícil mensuração. Por fim, serão propostas reflexões sobre o fortalecimento da autodeterminação informativa emocional, avaliando se os mecanismos vigentes são suficientes ou se a proteção da esfera mais íntima do indivíduo exige novas interpretações normativas e instrumentos adicionais.

Essa análise parte da premissa, consolidada ao longo do trabalho, de que a dignidade humana e o livre desenvolvimento da personalidade não podem ser compatíveis com um modelo em que a subjetividade do titular se converte em ativo econômico sem freios jurídicos eficazes. O desafio que se apresenta, portanto, não é apenas de adequação formal da lei, mas de construção de uma cultura protetiva capaz de acompanhar a sofisticação crescente da instrumentalização emocional nas plataformas digitais.

3.1 O PAPEL DA ANPD NA REGULAÇÃO DE TECNOLOGIAS DE RECONHECIMENTO EMOCIONAL

Diante da fragilidade do modelo de consentimento e da acentuada assimetria de poder entre controladores e titulares de dados emocionais, nesse contexto a Autoridade Nacional de Proteção de Dados (ANPD) assume o papel de núcleo essencial para a efetivação da autodeterminação informativa no Brasil. Diante disso, conforme a competência estabelecida no art. 55-J da Lei Geral de Proteção de Dados (LGPD), a Autoridade não atua apenas como entidade fiscalizadora, mas também como órgão responsável pela densificação normativa de conceitos abertos da lei. Nesse sentido, cabe à ANPD a tarefa de interpretar a natureza jurídica dos dados emocionais que, embora não citados explicitamente no rol do art. 5º, II, da LGPD, entende-se que derivam majoritariamente de tratamentos biométricos e comportamentais, o que os eleva à categoria de dados sensíveis sujeitos a um regime de proteção mais rigoroso.

A intervenção regulatória da ANPD torna-se indispensável para enfrentar o que a doutrina identifica como o risco da "caixa-preta"⁷ algorítmica. De acordo com o entendimento de Bioni (2019), a proteção de dados na modernidade exige uma transição do controle puramente individual para um modelo de governança institucionalizada.

Assim, a Autoridade deve exercer seu poder normativo para estabelecer esclarecimentos e garantias sobre a transparência algorítmica, impedindo que o segredo comercial das plataformas seja utilizado como subterfúgio para ocultar mecanismos de modulação comportamental que explorem a vulnerabilidade psíquica do usuário. A atuação da ANPD, portanto, deve focar na redução da opacidade dos sistemas de análise de sentimento, garantindo ao titular o direito à explicação e à compreensão do tratamento.

Sob a ótica da prevenção, a ANPD possui o instrumento do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como ferramenta de controle prévio de danos. Argumenta-se que tecnologias de reconhecimento emocional, por sua inerente invasão à esfera privada e seu potencial discriminatório, devem ser classificadas como atividades de alto risco. Segundo a perspectiva de Doneda (2006), a proteção da personalidade exige que o Estado intervenha

⁷ A metáfora da "caixa-preta" (*black box*) é utilizada na literatura de proteção de dados para descrever a opacidade dos sistemas de inteligência artificial e algoritmos de aprendizado de máquina (*machine learning*). O termo designa sistemas cujo funcionamento interno, lógica de processamento e critérios de decisão permanecem ocultos ao titular e às autoridades, permitindo apenas a observação dos dados de entrada (*inputs*) e dos resultados (*outputs*). Frank Pasquale (2015), em sua obra *The Black Box Society*, ressalta que essa invisibilidade é frequentemente protegida por direitos de propriedade intelectual e segredos comerciais, criando um cenário de assimetria informativa que dificulta o escrutínio de vieses discriminatórios e o exercício do direito à explicação.

para assegurar que o desenvolvimento tecnológico não ocorra à revelia da dignidade humana. Dessa forma, é imperativo que a Autoridade exija a realização de Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs)⁸ específicos para o uso de inteligências artificiais que tratam os dados sensíveis, condicionando a operação desses sistemas à demonstração explícita de medidas de mitigação de riscos e de respeito à integridade contextual do tratamento.

Ademais, a natureza disruptiva das tecnologias de reconhecimento emocional requer que a ANPD implemente modelos de governança que privilegiem a agilidade e a colaboração multissetorial. Conforme aponta o relatório de pesquisa coordenado por Junquilha et al. (2025), a regulação da inteligência artificial deve ser orientada por uma visão antropocêntrica, assegurando que o desenvolvimento técnico permaneça subordinado ao respeito inegociável à dignidade humana e aos direitos fundamentais. Nesse cenário, o uso de instrumentos como o *regulatory sandbox*⁹ (ambiente regulatório experimental) apresenta-se como uma estratégia eficaz para que a Autoridade monitore a aplicação de sistemas de inteligência artificial afetiva em contextos controlados, permitindo a identificação de riscos sistêmicos e vieses discriminatórios antes de sua escala comercial. Essa abordagem proativa fomenta um ecossistema de confiança, no qual a inovação é balizada pela transparência e pela constante prestação de contas perante a sociedade (Junquilha et al., 2025).

Por fim, a regulação exercida pela ANPD deve buscar harmonia com os padrões internacionais, em especial os diálogos estabelecidos com o regulamento europeu. A tendência global, refletida em legislações como o *AI Act*¹⁰ da União Europeia, aponta para restrições severas ou proibições do reconhecimento emocional em contextos de alta vulnerabilidade,

⁸O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o instrumento técnico e jurídico, previsto no art. 5º, inciso XVII, da LGPD, que consiste na 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. Trata-se de uma materialização do princípio da responsabilidade e prestação de contas (*accountability*), permitindo que a Autoridade Nacional de Proteção de Dados (ANPD) avalie a conformidade e a proporcionalidade de operações de alto risco, como o tratamento de dados biométricos e emocionais.

⁹O *regulatory sandbox*, ou ambiente regulatório experimental, consiste em um regime jurídico diferenciado no qual a autoridade reguladora permite que empresas testem inovações tecnológicas e modelos de negócios sob sua supervisão direta, em um ambiente controlado e por tempo determinado. Segundo Junquilha et al. (2025), esse instrumento é essencial para a regulação de tecnologias disruptivas, como a inteligência artificial, pois permite que o órgão regulador (no caso brasileiro, a ANPD) monitore riscos e impactos sociais em tempo real, fomentando a inovação sem abdicar da proteção aos direitos fundamentais e da transparência.

¹⁰ O *Artificial Intelligence Act* (AI Act), formalmente designado como Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, constitui o primeiro marco regulatório abrangente sobre inteligência artificial no mundo. O diploma adota uma abordagem baseada em níveis de risco (inaceitável, alto, limitado e mínimo) e é especialmente relevante para esta análise por estabelecer proibições ao uso de sistemas de reconhecimento de emoções em contextos específicos, como em locais de trabalho e instituições de ensino, servindo como paradigma para o desenvolvimento da regulação brasileira e para a atuação da ANPD.

como ambientes educacionais e laborais (Junquillo et al., 2025). No Brasil, a ANPD desempenha o papel de guia do mercado, devendo editar guias orientativos e resoluções que desestimulem a coleta indiscriminada de dados emocionais para fins puramente comerciais, preservando o que se define como privacidade emocional contra a total transparência do ser no meio digital.

3.2 A RESPONSABILIDADE CIVIL NO TRATAMENTO IRREGULAR DE DADOS EMOCIONAIS

A transição de uma sociedade informacional para um sistema movido pela inteligência artificial afetiva redefine as fronteiras da privacidade e tensiona as estruturas clássicas da responsabilidade civil no Direito brasileiro. Quando plataformas digitais realizam a captura, o processamento e a mercantilização de dados emocionais à revelia dos padrões de transparência, o ordenamento jurídico é provocado a responder a uma pergunta fundamental: como tutelar e reparar os danos decorrentes da intrusão na esfera mais íntima do ser humano? O enfrentamento dessa questão depara-se, de imediato, com a insuficiência dos mecanismos tradicionais baseados na culpa e na mensuração estritamente patrimonial do prejuízo, o que torna necessária a releitura do instituto a partir dos novos contornos dos direitos da personalidade.

Historicamente, o modelo de codificação civilista estruturou-se sob uma lógica de subsunção rígida e forte inclinação à reparação de danos visíveis (Schreiber, 2002). Essa abordagem torna-se anacrônica diante da velocidade e da invisibilidade das operações algorítmicas que caracterizam a economia da vigilância. No contexto dos dados emocionais, a verificação da culpa em sentido estrito — negligência, imprudência ou imperícia — constitui um obstáculo insuperável para o titular, pois o funcionamento interno dessas tecnologias permanece protegido pelo segredo comercial, consolidando a assimetria informativa e técnica que impede o titular de compreender a cadeia de processamento dos seus próprios dados (Pasquale, 2015; Junquillo et al., 2025).

A esse problema estrutural soma-se uma segunda camada de opacidade: a própria arquitetura de escolha das plataformas integra o conteúdo e o modo de fornecimento do serviço digital (Moreira; Duarte; Silva, 2026). Quando essa arquitetura é deliberadamente construída por meio de *dark patterns* — interfaces projetadas para induzir, confundir ou forçar decisões

contrárias ao interesse do usuário —, configura-se não apenas uma violação ética, mas um defeito estrutural e funcional do serviço na etapa pré-contratual, nos termos do art. 14, § 1º, do Código de Defesa do Consumidor (Verbicaro; Homci, 2024). A ilicitude não reside em um evento pontual ou em um erro acidental, mas na própria lógica econômica do serviço, o que afasta qualquer tentativa de enquadrá-la no modelo subjetivo de responsabilização.

Diante dessa dupla opacidade algorítmica, a aplicação do art. 186 do Código Civil cede espaço à principiologia protetiva integrada da LGPD e do CDC. O tratamento de dados sensíveis de cunho emocional não constitui atividade neutra, mas uma operação que carrega risco inerente aos direitos fundamentais (Bioni, 2019). Por essa razão, a responsabilidade civil assume natureza objetiva, fundamentada na teoria do risco criado: o controlador que auferir proveito econômico a partir da modulação comportamental dos usuários assume os bônus e os ônus dessa atividade, respondendo pelo dever de indenizar independentemente de elemento subjetivo doloso ou culposos, à luz do art. 42 da LGPD (Junquilho et al., 2025). Esse entendimento encontra respaldo também no horizonte normativo em formação, que sinaliza a consolidação legislativa da responsabilidade objetiva no campo da inteligência artificial.¹¹

Essa tendência normativa de imposição de deveres ativos às plataformas digitais ganhou concretude no ordenamento brasileiro com a edição dos Decretos Federais 12.975/2026 e 12.976/2026, de 20 de maio de 2026, que regulamentaram o Marco Civil da Internet à luz do entendimento fixado pelo Supremo Tribunal Federal nos Temas de Repercussão Geral 533 e 987 (Martins; Martins, 2026). O art. 16-B do Decreto 12.975/2026 instituiu regime de responsabilidade civil e administrativa fundado no "dever de cuidado" e na ocorrência de "falha sistêmica", definida como a não comprovação, pelo provedor, de condutas que assegurem os mais elevados níveis de segurança e que inibam a circulação massiva de conteúdos ilícitos. Trata-se de modelo que, tal como aqui defendido para o tratamento de dados emocionais, desloca o eixo da responsabilização da culpa individualizada para a omissão na gestão de riscos inerentes à atividade. Em reforço complementar, o Decreto 12.976/2026, voltado ao enfrentamento da violência de gênero em ambiente digital, positivou o dever de cuidado tecnológico das plataformas baseadas em inteligência artificial, impondo-lhes, nos arts. 9º e 10, a obrigação de implementar salvaguardas técnicas capazes de identificar e bloquear na origem

¹¹ O PL nº 2.338/2023 (Marco Civil da Inteligência Artificial), em tramitação no Senado Federal, prevê em seu art. 27 a responsabilidade integral do fornecedor ou operador de sistemas de IA pelos danos causados, independentemente do grau de autonomia, com culpa presumida nos casos de alto ou excessivo risco. Em paralelo, a Comissão de Juristas responsável pela revisão do Código Civil propôs, em anteprojeto, a inclusão do art. 932, inciso VII, para responsabilizar objetivamente os sujeitos que utilizem ou se beneficiem, direta ou indiretamente, de sistemas de inteligência artificial de alto risco.

a geração ou modificação não consentida de conteúdo íntimo — o que evidencia a extensão do dever de proteção também a dados de natureza sensível e emocional de titulares em situação de hipervulnerabilidade. Essa densificação regulatória recente corrobora empiricamente a direção proposta neste trabalho: a responsabilidade objetiva fundada no risco da atividade, somada a deveres proativos de proteção de grupos vulneráveis, consolida-se como vetor normativo dominante para a tutela de dados sensíveis no ambiente digital brasileiro.

A caracterização do nexo de causalidade e a configuração do dano permanecem, contudo, os desafios mais complexos. Em sistemas de análise de sentimento e perfilamento preditivo, as plataformas não buscam apenas observar o usuário, mas induzir comportamentos por meio do controle do fluxo informacional. Demonstrar o liame causal exato entre o monitoramento oculto dos estados de ânimo e uma decisão de consumo prejudicial é tarefa hercúlea para o cidadão comum, agravada pela hiperpersonalização das interfaces e pela testagem contínua de *layouts* por meio de testes A/B¹² (Pasquale, 2015; Moreira; Duarte; Silva, 2026). Nesse ponto, a tentativa das plataformas de invocar a imprevisibilidade algorítmica para romper o nexo causal não prospera juridicamente: ao optar pela implementação de sistemas de aprendizado contínuo (*machine learning*), o agente econômico assume os riscos dessa opacidade decisória, que configura fortuito interno inerente à atividade, incapaz, portanto, de excluir a responsabilidade (Mulholland, 2020).

Diante dessas assimetrias, impõe-se a aplicação sistemática da inversão do ônus da prova, autorizada pelo art. 42, § 2º, da LGPD, e pelo art. 6º, VIII, do CDC, cabendo ao agente econômico demonstrar a integridade, a licitude e a neutralidade de seus modelos algorítmicos (Siqueira; Moraes, 2022; Verbicaro; Homci, 2024). Ademais, para evitar que a fragmentação técnica da cadeia digital funcione como estratégia de dispersão de responsabilidade, a imputação jurídica deve pautar-se pela solidariedade de todos os integrantes que auferiram lucro com a operação, nos termos do art. 7º, parágrafo único, do CDC (Moreira; Duarte; Silva, 2026).

Por fim, a conceituação jurídica do prejuízo causado pela violação da privacidade emocional exige o abandono de visões estritamente patrimonialistas ou psicológicas. O dano moral, na vanguarda do direito civil contemporâneo, afasta-se de concepções que exigem a prova de dor ou sofrimento anímico e consiste, em verdade, na lesão direta a um atributo da

¹² Os testes A/B consistem em uma metodologia de experimentação contínua de interfaces digitais pela qual duas ou mais versões de um mesmo elemento — botão, cor, layout, ordem de exibição — são apresentadas simultaneamente a grupos distintos de usuários, a fim de identificar qual variante produz o comportamento mais favorável aos objetivos da plataforma. No contexto dos *dark patterns*, essa técnica é instrumentalizada para otimizar sistematicamente a capacidade manipulativa da interface, tornando a indução ao erro não um desvio accidental, mas o produto refinado de experimentação deliberada sobre as vulnerabilidades cognitivas do usuário (Moreira; Duarte; Silva, 2026).

personalidade humana (Schreiber, 2013). No plano digital, o prejuízo decorrente dos *dark patterns* e do perfilamento afetivo desdobra-se em uma tipologia multidimensional: o dano econômico direto, verificável em cobranças camufladas e armadilhas de assinatura; o dano informacional, caracterizado pelo esvaziamento da soberania sobre os próprios dados e escolhas; o dano moral autônomo, configurado pela violação à dignidade mediante subversão algorítmica da vontade; e o dano existencial, que emerge quando as arquiteturas de escolha são desenhadas para estimular gatilhos de compulsão e dependência comportamental (Verbicaro; Homci, 2024; Moreira; Duarte; Silva, 2026).

Essa lesão multidimensional atinge o que a doutrina conceitua como o "infinito particular" do ser humano — o espaço íntimo onde se formam emoções, pensamentos e convicções — e descaracteriza o isolamento essencial para o livre desenvolvimento da subjetividade (Cancelier, 2017). A extração oculta desse núcleo representa uma agressão direta à integridade psíquica e à dignidade, na medida em que retira do indivíduo o controle sobre os modos de construção da própria esfera privada (Sousa; Silva, 2020). Portanto, o tratamento irregular de dados emocionais por meio de padrões obscuros configura um dano moral *in re ipsa*: a lesão se consuma no exato instante em que a autodeterminação informativa é vulnerada pelo desenho manipulativo da plataforma, sendo desnecessária a comprovação de abalo psicológico para que surja o dever de reparar.

3.3 PROPOSTAS PARA O FORTALECIMENTO DA AUTODETERMINAÇÃO INFORMATIVA EMOCIONAL

Para proteger a privacidade emocional, o Direito precisa ir além do diagnóstico dos problemas e apresentar soluções práticas. Como compreendido, o consentimento individual tornou-se uma ilusão fática, e a responsabilidade civil auxilia apenas após o acontecimento do dano, o que é insuficiente para resguardar os dados emocionais dos usuários e seu livre desenvolvimento da personalidade. Por isso, garantir o controle sobre os próprios dados não pode ser uma responsabilidade exclusiva dos titulares diante da assimetria da relação destes com as plataformas. Essa proteção deve se tornar uma exigência real e estrutural, dividida entre regras claras de conduta para as empresas e uma fiscalização ativa por parte do órgão responsável.

Essa insuficiência do consentimento individual encontra respaldo, ainda, na literatura da economia comportamental, que desconstrói o pressuposto liberal do *homo economicus*¹³ subjacente ao modelo consensual. Conforme sistematizam Verbicaro e Calandrini (2022), os indivíduos operam sob racionalidade limitada, valendo-se de heurísticas — atalhos cognitivos que reduzem o esforço de decisão em detrimento da ponderação racional entre riscos e benefícios. Richard Thaler, como apontam Verbicaro e Calandrini (2022), evidencia que os usuários tendem a priorizar o benefício imediato do acesso a um produto ou serviço em detrimento da análise de longo prazo sobre a exposição de sua intimidade. Diante de dados emocionais — cuja natureza sensível os torna particularmente aptos a influenciar decisões de consumo —, esse déficit de capacidade decisória agrava-se, reforçando a conclusão de que o Estado deve assumir o papel de arquiteto das escolhas, convertendo a arquitetura das interfaces digitais em instrumento de proteção, e não de exploração, da vulnerabilidade algorítmica dos usuários.

Como primeira medida de contenção dogmática, faz-se imperativa a relativização da centralidade do consentimento como base legal padrão para o tratamento de dados emocionais. Conforme a classificação dos dados triviais sensibilizados defendida por Bioni (2019), a criação de perfis digitais dos usuários para inferir seus estados de ânimo desvirtua a finalidade original de registros digitais comuns, operando uma quebra da integridade contextual. Por essa razão, a Agência Nacional de Proteção de Dados (ANPD) deve editar resoluções que qualifiquem de forma estrita as hipóteses de tratamento dessas informações. Caso o controlador fundamente a atividade no legítimo interesse, deve ser exigido, de maneira compulsória, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) acompanhado de um teste de ponderação específico, apto a demonstrar que as expectativas legítimas de privacidade do usuário não foram violadas por mecanismos ocultos de modulação comportamental.

A base principal do fortalecimento da autodeterminação informativa, contudo, reside na adoção de uma abordagem baseada em risco que reconheça a existência de esferas sociais incompatíveis com o monitoramento afetivo automatizado. Existem contextos em que a assimetria de poder entre o agente de tratamento e o titular é tão acentuada que anula completamente a viabilidade de uma manifestação de vontade livre, tornando qualquer tentativa

¹³ O conceito de *homo economicus* (ou "Econ", na nomenclatura popularizada por Richard Thaler) constitui a premissa central da teoria econômica clássica, segundo a qual os indivíduos agiriam como agentes perfeitamente racionais, realizando escolhas imparciais por otimização e com o escopo inafastável de maximizar seu próprio bem-estar. No campo da Economia Comportamental, esse modelo abstrato é criticado por desconsiderar o fator humano, demonstrando-se empiricamente que os indivíduos reais operam sob o signo da racionalidade limitada e são guiados por atalhos mentais (heurísticas) que frequentemente conduzem a tomadas de decisões prejudiciais ou distantes da otimização teórica original (VERBICARO; CALANDRINI, 2022, p. 5).

de captação de dados emocionais uma afronta direta aos direitos da personalidade e à dignidade humana. Diante disso, propõe-se a delimitação normativa de "zonas proibidas"¹⁴, consistentes no banimento absoluto de tecnologias de reconhecimento emocional e perfilamento afetivo em setores de alta vulnerabilidade, com especial destaque para as relações de trabalho e o ambiente educacional (Schreiber, 2013).

Para além das zonas de proibição absoluta, nas esferas em que a exploração comercial de dados emocionais ainda seja considerada legítima — como no entretenimento e nas redes sociais —, o fortalecimento da autonomia exige a imposição do princípio do *Privacy by Default*¹⁵ (privacidade por padrão). Alinhando-se à crítica de Bioni (2019) sobre a manipulação do consentimento, e valendo-se das premissas de Thaler e Sunstein (2008) a respeito do impacto das opções padrão na arquitetura de escolha, propõe-se determinar por via regulamentar que qualquer funcionalidade dependente de biometria comportamental ou análise de sentimento venha desativada na configuração original do sistema. Com isso, desloca-se o ônus da configuração: o usuário não precisará mais percorrer percursos complexos criados por *dark patterns* para resguardar sua intimidade; caberá à plataforma o dever de solicitar uma permissão específica, isolada e destacada caso o titular opte, de forma afirmativa, por permitir o processamento de suas reações afetivas.

Essa proposta encontra respaldo doutrinário mais amplo na formulação de Ann Cavoukian sobre o *Privacy by Design*, estruturada em sete princípios fundacionais que, aplicados à privacidade emocional, oferecem parâmetros técnicos e regulatórios concretos para a concepção dos produtos e serviços digitais: (i) proatividade, não reatividade, e prevenção, não remediação, pela qual o risco de captura indevida de estados emocionais deve ser antecipado e evitado antes de sua ocorrência; (ii) privacidade como configuração padrão, assegurando que qualquer funcionalidade de reconhecimento emocional permaneça desativada até manifestação

¹⁴ A expressão "zonas proibidas" (*sphärengedanke*) remete à teoria das esferas da privacidade, de matriz germânica, que estratifica a vida íntima do indivíduo em graus de isolamento. A zona proibida — ou esfera do segredo e da intimidade profunda — representa o núcleo intangível da personalidade humana, refratário a qualquer intromissão externa do Estado ou de agentes privados. No ambiente digital, os sistemas de inteligência artificial que pretendem decodificar e monitorar os estados emocionais dos indivíduos operam uma violação direta a esse reduto inviolável, convertendo o foro íntimo e a subjetividade em ativos comerciais escrutináveis, o que confronta diretamente a cláusula geral de tutela da dignidade humana (SCHREIBER, 2013).

¹⁵ O princípio do *Privacy by Default* (privacidade por padrão) estabelece que as configurações de qualquer plataforma digital devem garantir, de forma automática e sem necessidade de intervenção ativa do usuário, o nível máximo de restrição regulatória e a limitação da coleta de dados ao estritamente necessário para a execução do serviço. O conceito integra a metodologia do *Privacy by Design*, desenvolvida originalmente por Ann Cavoukian na década de 1990, e encontra-se hoje expressamente positivado no artigo 25, § 2º, do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. No modelo brasileiro, a sua incorporação regulatória é defendida como mecanismo essencial para neutralizar os desvios da arquitetura de escolha e mitigar a vulnerabilidade do titular diante do perfilamento automatizado (Bioni, 2019).

afirmativa do titular; (iii) privacidade incorporada ao próprio *design*, e não acrescentada posteriormente como camada corretiva; (iv) funcionalidade integral, numa lógica de soma positiva que rejeita a falsa dicotomia entre inovação tecnológica e proteção da esfera emocional; (v) segurança de ponta a ponta, com proteção do dado emocional durante todo o seu ciclo de vida, da coleta ao descarte; (vi) visibilidade e transparência, que exigem a abertura dos critérios e da lógica de funcionamento dos sistemas de análise de sentimento aos titulares e às autoridades fiscalizadoras; e (vii) respeito pela privacidade do usuário, mantendo a arquitetura do sistema centrada nos interesses do titular dos dados (Cavoukian, 2011). A adoção desses princípios pela ANPD, por meio de resolução técnica, conferiria maior densidade normativa à exigência de que a privacidade emocional seja tratada como padrão originário do sistema, e não como opção residual a ser conquistada pelo titular.

A fixação de padrões *default* favoráveis à privacidade, todavia, não é suficiente caso não se enfrente, de forma específica, a arquitetura que lhe é oposta: os *sludges* digitais, notadamente os *dark patterns*. Cunhado por Harry Brignull em 2010, o termo designa os padrões obscuros de interface que induzem o consumidor a agir contra sua real preferência, valendo-se de técnicas como o *confirmshaming*, a *trick question* e o *roach motel*¹⁶, conforme classificação sistematizada por Verbicaro e Calandrini (2022). A gravidade dessas práticas é demonstrada empiricamente pelo experimento de Laguri e Strahilevitz (2021), relatado por Verbicaro e Calandrini (2022): a exposição de quase dois mil participantes a padrões obscuros agressivos elevou em 371% a adesão a um programa de tratamento de dados, em comparação ao grupo de controle não manipulado. Diante disso, propõe-se que a regulamentação do *Privacy by Default* seja acompanhada da tipificação, pela ANPD, das práticas de *dark patterns* como violação do dever de boa-fé objetiva no tratamento de dados emocionais, sob pena de a inversão do padrão de configuração ser neutralizada por artifícios de interface que reconduzam o titular, por indução, ao consentimento indesejado.

Nessa mesma linha, a instituição de *nudges* e do *Privacy by Design* no tratamento de dados emocionais não precisa restringir-se à atuação da ANPD sob fundamento exclusivo da

¹⁶ Trata-se de espécies de *dark patterns* (padrões obscuros de interface) que operam como manipulações comportamentais (*sludges*) no ciberespaço: o *confirmshaming* (ou confirmação-vergonha) manifesta-se quando a plataforma tenta constranger emocionalmente o consumidor no momento de uma recusa ou cancelamento, moldando as opções de modo a associar a negação a uma escolha prejudicial ou irresponsável do próprio titular (enquadrando a decisão de declinar como um desinteresse em proteger os próprios dados); a *trick question* configura-se como uma pergunta-truque com redação sinuosa, ambígua ou intencionalmente confusa, projetada para induzir o usuário ao erro no momento de selecionar a alternativa de rejeição; e o *roach motel* (ou motel de baratas) caracteriza-se pela intencional assimetria de fluxos da interface, estruturada de forma a tornar o percurso de desvinculação, exclusão ou cancelamento de um serviço consideravelmente mais complexo, burocrático e oneroso do que o ato imediato de adesão (VERBICARO; CALANDRINI, 2022, p. 9).

LGPD. Em coerência com o diálogo integrado de fontes normativas adotado ao longo deste trabalho, reconhece-se na Política Nacional das Relações de Consumo — PNRC, prevista nos artigos 4º e 5º do Código de Defesa do Consumidor (Brasil, 1990) — um vetor complementar de intervenção estatal, na medida em que autoriza o Estado a atuar como "arquiteto de escolhas" para a harmonização das relações de consumo digitais e para a proteção da vulnerabilidade do consumidor (Verbicaro; Calandrini, 2022). Assim, a Secretaria Nacional do Consumidor (SENACON) poderia atuar de forma coordenada com a ANPD na fiscalização de práticas manipulativas envolvendo dados emocionais, conferindo maior efetividade e capilaridade institucional às propostas ora defendidas, sem prejuízo da competência sancionatória própria da ANPD nos termos do artigo 52 da LGPD.

Como exemplo de *nudge* especificamente aplicável à proteção de dados emocionais, cogita-se a utilização de códigos cromáticos em avisos de privacidade, destacando finalidade, ciclo de vida e grau de sensibilidade do dado coletado. Estudos sobre a influência da cor no comportamento do consumidor, conforme relatam Verbicaro e Calandrini (2022), com base em Guimarães (2000) e Crepaldi (2006), demonstram sua aptidão para captar a atenção do titular no momento da decisão, o que sugere um instrumento de baixo custo regulatório e alto potencial informativo para reforçar, no momento da coleta, a natureza sensível dos dados emocionais.

Em suma, as propostas de atuação da ANPD e, subsidiariamente, da Secretaria Nacional do Consumidor (SENACON) — na fixação de limites rígidos para as bases legais, no banimento de tecnologias afetivas em contextos de subordinação, na inversão do desenho das interfaces mediante o *Privacy by Default* e o *Privacy by Design*, e no combate específico às *dark patterns* — formam um conjunto harmônico de medidas preventivas, fundado no diálogo entre a LGPD e o Código de Defesa do Consumidor. Somente por meio dessa intervenção estrutural multissetorial o ordenamento jurídico brasileiro será capaz de retirar a autodeterminação informativa do plano meramente simbólico, conferindo eficácia real à tutela da dignidade humana e ao livre desenvolvimento da personalidade na era da inteligência artificial.

CONSIDERAÇÕES FINAIS

A nova sociedade regida pela inteligência artificial e pela consolidação da economia da vigilância exige do Direito muito mais do que a mera aplicação objetiva de seus institutos tradicionais; demanda uma postura ativa de salvaguarda da própria essência da dignidade humana. A presente pesquisa dedicou-se a investigar os limites jurídicos da coleta e do tratamento de dados emocionais por plataformas digitais sob a ótica da legislação brasileira, bem como em que medida a arquitetura de escolha dessas plataformas compromete a autodeterminação informativa e o livre desenvolvimento da personalidade do titular. Os resultados alcançados confirmam que a extração e a mercantilização automatizada da subjetividade humana colocam em risco o núcleo intangível dos direitos da personalidade, e que apenas um diálogo integrado entre a LGPD, o Código Civil e o Código de Defesa do Consumidor é capaz de conferir densidade normativa suficiente a essa proteção.

Ao longo do desenvolvimento deste estudo, tornou-se evidente que o modelo clássico de proteção de dados, excessivamente centrado na figura do consentimento individual, tornou-se uma ilusão fática diante da profunda assimetria técnica e informativa que separa as corporações tecnológicas dos titulares de dados. A complexidade dos algoritmos de captação e processamento de dados, frequentemente resguardada sob a faculdade do segredo comercial, inviabiliza a compreensão da cadeia de tratamento pelo cidadão comum. Constatou-se, ainda, que a arquitetura de escolha das plataformas — não raro estruturada por meio de *dark patterns* — opera uma grave quebra da integridade contextual, desvirtuando a finalidade original dos registros digitais e esvaziando a capacidade de escolha do indivíduo sobre sua própria intimidade.

Diante desse cenário de vulnerabilidade estrutural, a presente pesquisa demonstrou a insuficiência dos mecanismos civilistas tradicionais baseados na culpa e na mensuração puramente patrimonial do prejuízo gerado pelas plataformas. Como resposta dogmática a essa lacuna, concluiu-se que a responsabilidade civil no tratamento irregular de dados emocionais assume natureza essencialmente objetiva, fundamentada na teoria do risco criado: aquele que auferir proveito econômico a partir da modulação comportamental e do perfilamento afetivo dos titulares deve assumir os ônus e os benefícios de sua atividade. Sob a mesma perspectiva, o dano causado pela intrusão na privacidade emocional afasta-se de visões que exigem a prova objetiva de dor ou sofrimento anímico: a violação consuma-se na lesão direta a um atributo da personalidade e na quebra do controle sobre o fluxo informativo, configurando dano moral *in*

re ipsa, cujo dever de reparar surge no exato instante em que a autodeterminação informativa é vulnerada.

Para além do diagnóstico crítico, o presente trabalho cumpriu o seu propósito de apresentar soluções práticas e preventivas voltadas a conferir eficácia real à tutela jurídica dos dados emocionais. O fortalecimento da autodeterminação informativa exige uma virada de postura da Autoridade Nacional de Proteção de Dados (ANPD), que deve classificar as tecnologias de reconhecimento emocional como atividade de alto risco, condicionando sua operação à elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs) e ao monitoramento por meio de *regulatory sandboxes*. Propôs-se, ainda, a imposição regulatória do princípio do *Privacy by Default* — garantindo que qualquer funcionalidade de análise de sentimento venha desativada na configuração original do sistema — e a adoção de uma abordagem baseada em risco que reconheça a existência de "zonas proibidas", consistentes no banimento absoluto dessas tecnologias em setores de extrema subordinação, como as relações de trabalho e o ambiente educacional. Tal proposta encontra respaldo no diálogo com padrões internacionais, notadamente o *AI Act* europeu, que já trilha caminho semelhante de restrição severa ao reconhecimento emocional em contextos de alta vulnerabilidade.

Em suma, as conclusões desta pesquisa convergem para a certeza de que a proteção ao âmbito de intimidade do ser humano e ao seu direito de isolamento psíquico não pode ser convertida em ônus exclusivo do polo vulnerável da relação. Somente por meio de uma intervenção estrutural — que articule a responsabilidade civil objetiva, a inversão sistemática do ônus da prova e uma regulação preventiva rígida por parte da ANPD — o ordenamento jurídico brasileiro será capaz de retirar a autodeterminação informativa do plano meramente simbólico. Salvaguardar a privacidade emocional na era da inteligência artificial é, fundamentalmente, garantir que o avanço tecnológico não se curve ao esvaziamento da intimidade emocional e que o livre desenvolvimento da personalidade permaneça um direito inalienável de cada indivíduo.

REFERÊNCIAS

BRANDEIS, Louis D.; WARREN, Samuel D. O direito à privacidade. Tradução por: Maria Clara de Souza Seixas e Marcus Seixas Souza. Revista de Direito Civil Contemporâneo, vol. 38, ano 11, p. 391-417. São Paulo: Ed. RT, jan./mar. 2024.

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

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

BOHRER, Igor Graeff. A proteção de dados pessoais como direito da personalidade e seu risco diante do online profiling. 2019. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2019.

CANCELIER, Mikhail Vieira de Lorenzi. Infinito particular: privacidade no século XXI e a manutenção do direito de estar só. Rio de Janeiro: Lumen Juris, 2017.

JUNQUILHO, T. A.; MENDES, L. S. F.; MEIER, I. F.; SILVA, C. C. da (coord.). Relatório de pesquisa: A regulação da Inteligência Artificial: Tendências regulatórias globais. Brasília: Laboratório de Governança e Regulação de Inteligência Artificial (LIA) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), 2025. Disponível em: <https://repositorio.idp.edu.br/handle/123456789/5608> . Acesso em: 14/05/2026.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

SCHREIBER, Anderson. Direitos da Personalidade. 2. ed. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. Os Direitos da Personalidade e o Código Civil de 2002. In: **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 3, n. 11, p. 3-28, jul./set. 2002.

SIQUEIRA, Dirceu Pereira; MORAIS, Fausto Santos de. Do reconhecimento da autodeterminação informativa como direito da personalidade e do princípio da segurança. *Revista Direito e Debate*, Ijuí, ano XXXI, n. 57, jan./jun. 2022.

SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. Proteção de dados pessoais e os contornos da autodeterminação informativa. *Relato de Pesquisa*, [S. l.], p. 1-14, 2020.

VERBICARO, Dennis; HOMCI, Janaina Vieira. A responsabilidade civil por padrões obscuros estruturados por modelos algorítmicos. *Revista de Direito do Consumidor*, vol. 156, ano 33, p. 165-181, São Paulo: Ed. RT, nov./dez. 2024.

MOREIRA, Amanda Oliveira da Câmara; DUARTE, Luisa Ferreira; SILVA, Leonardo Rocha da. Responsabilidade civil no contexto de padrões obscuros e modelos algorítmicos. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 31, ano 9, abr./jun. 2026.

CASTRO, Júlia Ribeiro de. O direito fundamental à privacidade mental. *Revista de Direito e as Novas Tecnologias*, São Paulo, v. 27, ano 8, abr./jun. 2025.

DIAS, Clara Angélica Gonçalves Cavalcanti; MELO, Bricio Luis da Anunciação. A autodeterminação informativa como manifestação do direito à privacidade. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 37, ano 10, p. 51-75, out./dez. 2023.

MARTINS, Fernando Rodrigues. "Neurolaw", neurodireitos e comércio eletrônico como lacunas éticas no sistema jurídico. Por uma metodologia do direito digital: nove diretrizes para sobrepor a autorregulação algorítmica pela regulação humana. *Revista de Direito do Consumidor*, São Paulo, v. 154, ano 33, p. 191-217, jul./ago. 2024.

DORETO, João Victor Vieira; BORGES, Grazielly Almeida; FERREIRA, Keila Pacheco. A exploração de vulnerabilidades por inteligência artificial na publicidade personalizada. *Revista de Direito do Consumidor*, São Paulo, v. 164, ano 35, p. 15-36, mar./abr. 2026.

HOLANDA, Fábio Campelo Conrado de; COSTA, Ari Batista Macêdo. Publicidade oculta, design persuasivo e neurovulnerabilidade: as práticas comerciais dirigidas a crianças e

adolescentes nas redes sociais. *Revista de Direito do Consumidor*, São Paulo, v. 163, ano 35, p. 59-79, jan./fev. 2026.

MADALENA, Juliano. A vulnerabilidade digital da pessoa e da coisa. *Revista de Direito do Consumidor*, São Paulo, v. 162, ano 34, p. 247-271, nov./dez. 2025.

MARQUES, Claudia Lima; MARTINS, Fernando Rodrigues. A proteção dos dados pessoais, o mundo digital e o pioneirismo do Código de Defesa do Consumidor: uma homenagem a Danilo Doneda. *Revista de Direito do Consumidor*, São Paulo, v. 152, ano 33, p. 41-57, mar./abr. 2024.

MARQUES, Claudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. *Revista de Direito do Consumidor*, São Paulo, v. 145, ano 32, p. 295-316, jan./fev. 2023.

VERBICARO, Dennis; CALANDRINI, Jorge. Nudges na proteção de dados pessoais no ciberespaço: um empurrão para incentivar decisões racionais dos consumidores. *Revista de Direito do Consumidor*, São Paulo, v. 142, a. 31, p. 185-214, jul./ago. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01/06/2026

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidente da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 01/06/2026

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidente da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2002/110406compilada.htm. Acesso em: 01/06/2026

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 01/06/2026.

BRASIL. Decreto nº 12.975, de 20 de maio de 2026. e BRASIL. Decreto nº 12.976, de 20 de maio de 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12975.htm . Acesso em: 17 jul. 2026.

MARTINS, Fernando Rodrigues; MARTINS, Miguel Cabral de Araújo. Redesenho regulatório das esferas digitais, a partir dos recentes Decretos Federais 12.975 (MCI) e 12.976 (violência de gênero), de 2026. Aperfeiçoando o sistema de responsabilidade civil das Big Techs em promoção aos vulneráveis e em legitimação ao exercício da liberdade de expressão. Boletim Revista dos Tribunais Online, vol. 75, maio 2026, DTR\2026\8178.

BAUMAN, Zygmunt; LYON, David. Vigilância líquida. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

ZANATTA, Rafael A. F. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. 2019.

CAVOUKIAN, Ann. Privacy by Design. Toronto: Information and Privacy Commissioner of Ontario, Canada, 2009.

PICARD, Rosalind W. Affective Computing. Cambridge, MA: MIT Media Laboratory, Perceptual Computing Section, Technical Report n. 321, 1995. Disponível em: <https://arl.human.cornell.edu/linked%20docs/Picard%20Affective%20Computing.pdf>. Acesso em: 17 jul. 2026.