DIREITO DIGITAL

REFORMA DO CÓDIGO CIVIL: UM ESTUDO COMPARADO DO DIREITO CIVIL DIGITAL

AGOSTO | 2025

COORDENAÇÃO
LUIS FELIPE SALOMÃO
ELTON LEME

COORDENAÇÃO CIENTÍFICA
LAURA PORTO

FGV JUSTIÇA

ISBN 978-65-83308-82-5

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
(CÂMARA BRASILEIRA DO LIVRO, SP, BRASIL)

Direito digital [livro eletrônico] : reforma do
código civil : um estudo comparado do direito
civil digital / coordenação Luis Felipe
Salomão, Elton Leme ; coordenação científica
Laura Porto. -- Rio de Janeiro : Fundação
Getulio Vargas, 2025.
PDF
Bibliografia.
ISBN 978-65-83308-82-5
1. Código civil 2. Direito digital
3. Responsabilidade civil I. Salomão

25-290579 CDU-374.51

ÍNDICES PARA CATÁLOGO SISTEMÁTICO:

1. Direito digital : Direito civil 374.51

Cibele Maria Dias - Bibliotecária - CRB-8/9427

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

A

APRESENTAÇÃO

A FGV Justiça tem como missão identificar, entender, sistematizar, desenvolver e aprimorar soluções voltadas ao aperfeiçoamento do sistema de justiça. Atualmente, a FGV Justiça conta com as seguintes linhas de pesquisa: (1) Governança Digital e Inovação; (2) Sustentabilidade e Responsabilidade Social; (3) Democracia; (4) Direitos Humanos; (5) Solução de Conflitos; (6) Saúde; (7) Infraestrutura e (8) Finanças Públicas e Tributação e (9) Penal.

O presente estudo é desenvolvido no âmbito da linha de pesquisa "Governança Digital e Inovação", que trata de temas relacionados à transformação e à governança digital.

O Projeto de Lei nº 4, de 2025, de autoria do senador Rodrigo Pacheco, dispõe sobre a atualização da Lei nº 10.406, de 10 de janeiro de 2022 (Código Civil) e da legislação correlata. O texto do projeto de lei é fruto do trabalho da Comissão de Juristas, responsável pela revisão e atualização do Código Civil, instituída pelo Senado Federal. A referida comissão foi presidida por mim e pelo vice-presidente, o ministro do Superior Tribunal de Justiça (STJ) Marco Aurélio Bellizze. Além disso, teve como relatores-gerais o professor Flávio Tartuce e a professora Rosa Maria de Andrade Nery.

A proposta da Comissão de Juristas visou atualizar o texto do Código Civil à jurisprudência já pacificada pelo Supremo Tribunal Federal (STF), pelo Superior Tribunal de Justiça (STJ) e pelas Jornadas de Direito Civil realizadas pelo Conselho da Justiça Federal (CJF). Entre as modificações, houve a proposta de criação do Livro Direito Civil Digital, que preenche uma lacuna normativa e foi concebido com o objetivo de harmonizar o Direito Civil com a era digital. A subcomissão responsável pelo Livro Direito Civil Digital teve como sub-relatora Laura Porto, coordenadora científica deste estudo e, como membros, Dierle Nunes e Ricardo Campos.

O avanço acelerado das tecnologias digitais no século XXI tem provocado uma transformação estrutural nas formas de comunicação, interação social e realização de negócios. Dados apresentados neste estudo indicam que a conexão à internet já alcança mais de dois terços da população mundial, e que há um crescimento expressivo no uso de redes sociais e no comércio eletrônico. Os dados referentes ao Brasil demonstram que o país segue a tendência mundial, com crescente penetração da internet e das mídias digitais nos atos da vida cotidiana.

Diante desse cenário, o Direito Civil ocupa posição central nesse debate, em especial, no que se refere à regulação do Direito Digital. No direito brasileiro, apesar da existência de normas específicas, tais como o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados (LGPD), ainda persistem lacunas que precisam ser supridas pelas normas civis. Desta forma, se faz necessária a atualização normativa, que o legislador pretende atender por meio da inclusão de um novo livro no âmbito do projeto de reforma Código Civil, dedicado a regular o Direito Civil Digital.

Trata-se, portanto, de uma proposta inovadora no contexto dos ordenamentos jurídicos, concebida para enfrentar os desafios normativos decorrentes da digitalização das relações contemporâneas. O projeto busca sistematizar e consolidar um arcabouço normativo a partir de um conjunto de princípios, direitos e deveres aplicáveis ao ambiente digital, regulando temas como direito à desindexação de conteúdos e à exclusão de dados ou informações; neurodireitos; plataformas digitais e moderação de conteúdo; patrimônio digital; presença e identidade de crianças e adolescentes no ambiente digital; inteligência artificial; contratos celebrados por meios digitais; assinaturas eletrônicas e atos notariais eletrônicos – E-Notariado.

Além disso, o novo livro irá "dialogar" com os outros institutos do Direito Civil, previstos nos demais livros e normativos.

Este estudo explora o impacto das transformações no ambiente digital e os desafios enfrentados na tentativa de regulamentá-lo a partir da análise das propostas presentes no Livro Direito Civil Digital no âmbito da reforma do Código Civil. Entre os temas tratados pela reforma do Código Civil no Livro Direito Civil Digital, este estudo analisará: a) Pessoa no ambiente digital: desindexação e exclusão de dados ou informações; b) Pessoa no ambiente digital: neurodireitos; c) Direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo; d) Patrimônio digital; e) Presença e identidade de crianças e adolescentes no ambiente digital; f) Inteligência artificial; g) Celebração de contratos por meios digitais e h) Assinaturas eletrônicas.

A pesquisa foi desenvolvida a partir de: a) revisão bibliográfica, a fim de compreender as abordagens teóricas e práticas atuais; b) estudos de casos concretos, nos quais se destacam conflitos e questões legais decorrentes do ambiente digital, avaliando como o Direito Civil tem sido aplicado e identificando as oportunidades de aprimoramento; c) identificação de experiências normativas estrangeiras no âmbito das temáticas investigadas, extraindo lições e práticas que possam ser aplicadas no contexto brasileiro.

Os dados da pesquisa foram consolidados neste estudo com o intuito de oferecer um panorama sobre como o tema é tratado no âmbito da reforma do Código Civil e na experiência normativa de outros países.

LUIS FELIPE SALOMÃO
Ministro do Superior Tribunal
de Justiça (STJ), Coordenador da
FGV Justiça e Presidente da Comissão
de Juristas para a Reforma do Código Civil

INTRODUÇÃO

01

1 INTRODUÇÃO

1.1 Objetivo geral

Este estudo se insere na linha de pesquisa "Governança Digital e Inovação" e objetiva analisar as propostas de regulamentação do Direito Civil Digital no âmbito da reforma do Código Civil. Entre os temas tratados pela reforma do Código Civil no Livro Direito Civil Digital, este estudo analisará:

• Pessoa no ambiente digital: desindexação e exclusão de dados ou informações;

• Pessoa no ambiente digital: neurodireitos;

• Direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo;

• Patrimônio digital;

• Presença e identidade de crianças e adolescentes no ambiente digital;

• Inteligência artificial;

• Celebração de contratos por meios digitais;

• Assinaturas eletrônicas.

1.2 Objetivos específicos

a) Explorar o panorama normativo a fim compreender o estado atual da legislação no Brasil, identificando lacunas que necessitam de atualização;

b) Analisar a proposta de regulamentação constante do Projeto de Lei nº 4, de 2025;

c) Realizar uma revisão abrangente da doutrina, visando compreender as abordagens teóricas e práticas existentes;

d) Estudar casos concretos, nos quais se destacam conflitos e questões legais emergentes no ambiente digital, avaliando como o Direito Civil tem sido aplicado e identificando oportunidades de aprimoramento;

e) Identificar experiências normativas estrangeiras no âmbito das temáticas investigadas, extraindo lições e práticas que possam ser aplicadas no contexto brasileiro.

1.3 Metodologia

Este estudo foi desenvolvido por meio das seguintes abordagens metodológicas:

a) Revisão bibliográfica, a fim de compreender as abordagens teóricas e práticas atuais;

b) Análise documental, com o objetivo de detalhar as lacunas na legislação atual e as mudanças propostas;

c) Estudos de caso, para identificar como os casos concretos que envolvem questões legais emergentes no ambiente digital têm sido solucionados pela doutrina e pela jurisprudência;

d) Pesquisa de experiências normativas estrangeiras relacionadas às temáticas do estudo com o objetivo de comparar essas experiências com o contexto brasileiro e extrair lições e práticas que possam ser aplicadas.

1.4 Organização

O estudo divide-se em quatro partes principais. Nesta primeira, introdutória, são apresentados seus objetivos e a metodologia. O segundo capítulo apresenta o contexto de elaboração do estudo – nomeadamente, o processo de digitalização da sociedade e os impactos das transformações tecnológicas sobre o direito, dentre os quais está a necessidade de criação de um livro destinado especificamente à regulação do Direito Civil Digital, no âmbito do projeto de reforma do Código Civil Brasileiro.

O terceiro capítulo é dedicado ao estudo pormenorizado das disposições do Livro Direito Civil Digital, abordando seus aspectos centrais, tanto de maneira descritiva quanto crítica. São abordados os aspectos teóricos, bem como os dispositivos legais que foram analisados conforme a ordem em que foram originalmente apresentados no Projeto de Lei nº 4, de 2025, respeitando, inclusive, a numeração presente na versão apresentada.

O último capítulo, de natureza conclusiva, apresenta uma avaliação geral das inovações propostas no Livro Direito Civil Digital, além de observações sobre eventuais aprofundamentos que se revelarem necessários.

1.5 Rede de pesquisa institucional

1.5.1 Coordenação científica da pesquisa

Laura Porto

Advogada e sub-relatora da Subcomissão de Direito Digital para a reforma do Código Civil (Senado Federal, 2023-2024). Especialista em Direito Digital e Proteção de Dados. Mestranda no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Professora da pós-graduação da Escola Superior de Advocacia (ESA/OAB) e da Escola Nacional da Magistratura (ENM).

1.5.2 Pesquisadores

Renata Braga

Pós-doutora pela Universidade Federal do Rio de Janeiro (UFRJ)/Universidade de Coimbra. Doutora em Direito pela Universidade Federal de Santa Catarina (UFSC). Mestra em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professora associada do curso de Direito da Universidade Federal Fluminense (UFF – Volta Redonda). Coordenadora do Grupo de Estudos e Pesquisa em Métodos Consensuais de Solução de Conflitos e do Observatório de Direito e Tecnologia da UFF – Volta Redonda. Pesquisadora colaboradora da FGV Justiça.

Samuel Rodrigues de Oliveira

Doutor em Teoria do Estado e Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Mestre em Direito e Inovação e bacharel em Direito pela Universidade Federal de Juiz de Fora (UFJF). Advogado e pesquisador da FGV Justiça.

Camila Thiebaut Bayer Lannes

Advogada e pesquisadora da FGV Justiça. Doutoranda, mestra e bacharela em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em Direito Ambiental e Minerário pelo Centro Universitário São Camilo.

Juliana Justo Botelho Castello

Professora titular de Processo Civil da Faculdade de Ensino Superior de Linhares (FACELI/ES). Doutora em Direito Processual pela Faculdade de Direito da Universidade de São Paulo (USP). Mestra em Direito Constitucional, na linha de Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV). Analista pesquisadora do CORE IA – Centro de Inovação e Inteligência Artificial do TJES. Membro da Associação Brasileira Elas no Processo (ABEP). Membro do Instituto de Direito Processual (IBDP).

Priscila Luz Barreiros

Graduada em Direito na Universidade de Frankfurt. Mestra pela Frankfurt University of Applied Sciences. Professora na Frankfurt University of Applied Sciences. Pesquisadora no Research Lab for Law and Applied Technologies.

Ana Beatriz da Silva Marques

Graduanda em Direito pela Universidade Federal Fluminense (UFF). Pesquisadora do Grupo de Pesquisa Observatório Direito e Tecnologia da UFF/VR.

Ana Beatriz dos Santos Taveira

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Ana Oliveira Mattos

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Davi de Souza Paulino

Graduado em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisador do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Elena Mello Silva de Paula

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia e do Grupo de Estudos em Meio Ambiente e Direito da UFF/VR.

Gabriela de Moraes Neves

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Gláucio da Silva Teixeira Júnior

Graduando em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisador do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

João Vitor Sampaio Nicolau de Castro Moreira

Graduando em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisador do Grupo de Pesquisa Observatório em Direito e Tecnologia da UFF/VR.

Luana Cristina de Oliveira

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Mariana Guerra Silveira

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Matheus dos Santos Caetano

Procurador do Estado de São Paulo. Graduado em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisador do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Nicole Rodrigues

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Thalita Dutra Ramos

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

Victória Oliveira Nazareth

Graduanda em Direito pela Universidade Federal Fluminense (UFF/VR). Pesquisadora do Grupo de Pesquisa Observatório de Direito e Tecnologia da UFF/VR.

CONTEXTUALIZAÇÃO

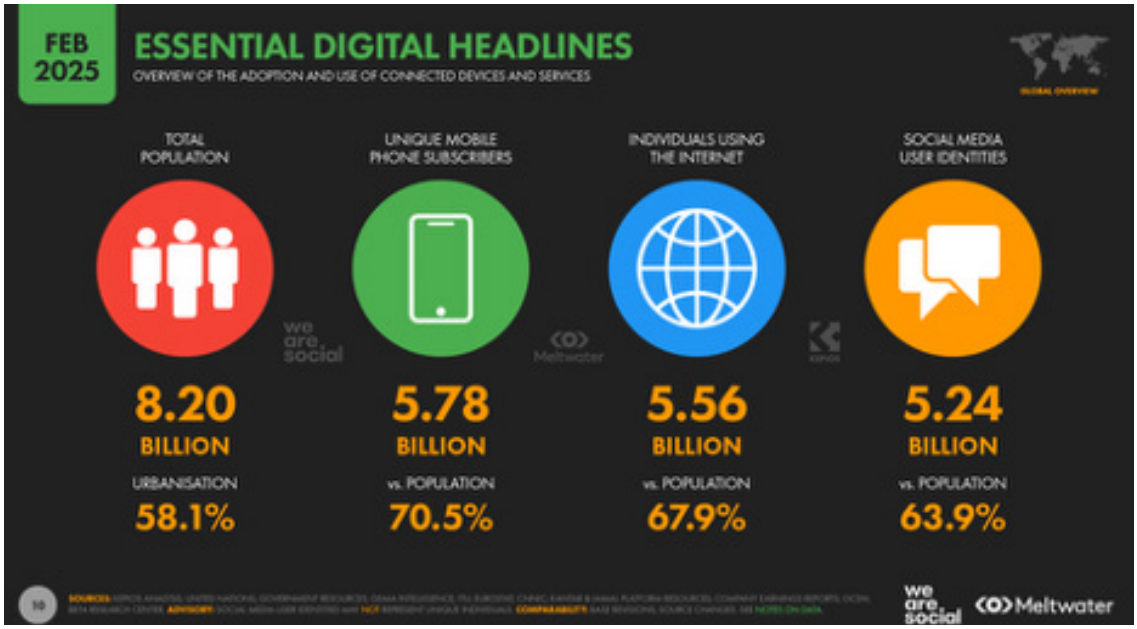
02

2. CONTEXTUALIZAÇÃO: A REFORMA DO CÓDIGO CIVIL E O LIVRO DIREITO CIVIL DIGITAL

2.1 Transformações tecnológicas e a digitalização da sociedade

O século XXI presenciou um acelerado desenvolvimento das tecnologias digitais com a expansão da conectividade em escala mundial e também das novas formas de circulação da informação (Castells, 2018). O relatório Digital 2025: Global Overview Report, elaborado pela We Are Social e Meltwater (2025) traça um panorama do estado da conectividade digital mundial, reunindo dados relevantes sobre usuários de internet, redes sociais e dispositivos móveis. Segundo o relatório, no mundo, a utilização do telefone celular soma 5,78 bilhões de pessoas, o que equivale a 70,5% da população total, enquanto um total de 5,56 bilhões de pessoas usam a internet, resultando em 67,9% da população total. Outro ponto de destaque se refere à utilização de redes sociais, que vem crescendo com, atualmente, 5,24 bilhões de perfis globais de usuários, que equivalem a 63,9% da população mundial.

Figura 1 – Dados gerais sobre o ambiente digital



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

O relatório trata também do crescimento do comércio eletrônico, com a estimativa de que o número de pessoas que fazem compras on-line de bens de consumo seja de cerca de 2,5 bilhões, movimentando mais de 4 trilhões de dólares.

Figura 2 – Dados sobre o *e-commerce*

Fonte: Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em 4 abr. 2025.

Ao trazer essas análises para o contexto brasileiro, com dados do início de 2025, o relatório aponta que:

• Há 217 milhões de conexões móveis celulares ativas no Brasil, porém algumas dessas conexões podem incluir apenas serviços como voz e SMS, e algumas podem não incluir acesso à internet.

• Há 183 milhões de indivíduos usando a internet no Brasil, o que representa 86,2% da população brasileira.

• Há 144 milhões de perfis de usuários de mídia social no Brasil, o que equivale a 67,8% da população total brasileira.

De acordo com Manuel Castells (2018), a sociedade em rede trouxe uma reestruturação de poder e da comunicação, atribuindo importância ainda maior à informação. O rápido avanço das tecnologias digitais e a digitalização crescente das relações sociais, econômicas e jurídicas têm trazido novos riscos e dilemas para o Direito contemporâneo. Como destaca o relatório Digital 2025: Global Overview Report, o ambiente digital já abrange mais de dois terços da população mundial, movimenta cifras bilionárias no comércio eletrônico e transforma profundamente as formas de interação entre as pessoas.

A universalização do acesso à internet e a crescente digitalização promoveram uma revolução em todas as esferas da vida, havendo "a necessidade de adequar os ordenamentos jurídicos para garantir a regulação e a proteção dos direitos em um ambiente cada vez mais conectado e globalizado" (Porto, 2025b, p. 387), pois "as soluções já existentes no ordenamento não mais respondem a diversas questões trazidas pela digitalização" (Porto, 2025b, p. 388). Nesse contexto, o Projeto de Lei nº 4, de 2025, de autoria do senador Rodrigo Pacheco, propõe a atualização da Lei nº 10.406, de 10 de janeiro de 2022 (Código Civil) e da legislação correlata. Entre as diversas modificações, como já ressaltado, houve a proposta de criação do Livro Direito Civil Digital, desenvolvida pela Subcomissão de Direito Digital para a Reforma do Código Civil, composta por Laura Porto, Dierle Nunes e Ricardo Campos. Segundo o ministro Luis Felipe Salomão: "Será um Código Civil para as gerações futuras, que terão de lidar com a transição da vida analógica para a digital" (Salomão, 2025, p. 17).

2.2 Do Direito Civil Digital

Como visto anteriormente, a inclusão de um novo livro no âmbito do projeto de reforma do Código Civil, dedicado a regular o chamado Direito Civil Digital, visa a preencher uma significativa lacuna normativa. O referido livro objetiva, assim, ser um eixo fundamental, evitando a desarticulação do sistema jurídico existente, a partir do estabelecimento de conceitos gerais que servirão de diretrizes para regulamentações futuras e outros temas e questões que possam surgir ao longo do tempo, encontrando-se dividido nos seguintes capítulos:

O referido livro objetiva, assim, ser um eixo fundamental, evitando a desarticulação do sistema jurídico existente, a partir do estabelecimento de conceitos gerais que servirão de diretrizes para regulamentações futuras e outros temas e questões que possam surgir ao longo do tempo, encontrando-se dividido nos seguintes capítulos:

> Capítulo I – Disposições gerais;
>
> Capítulo II – Da pessoa no ambiente digital;
>
> Capítulo III – Das situações jurídicas no ambiente digital;
>
> Capítulo IV – Do direito ao ambiente digital transparente e seguro;
>
> Capítulo V – Patrimônio digital;
>
> Capítulo VI – A presença e a identidade de crianças e adolescentes no ambiente digital;
>
> Capítulo VII – Inteligência artificial;
>
> Capítulo VIII – Da celebração de contratos por meios digitais;

Capítulo IX – Assinaturas eletrônicas; e

Capítulo X – Atos Notariais Eletrônicos – E-Notariado.

O primeiro capítulo do livro, intitulado "Disposições Gerais", estabelece conceitos jurídicos instrumentais para os demais capítulos. Estabelece-se, de imediato, que o Direito Civil Digital "visa a fortalecer o exercício da autonomia privada, a preservar a dignidade das pessoas e a segurança de seu patrimônio, bem como apontar critérios para definir a licitude e a regularidade dos atos e das atividades que se desenvolvem no ambiente digital" (art. 2.027-A). O "ambiente digital" corresponde, para os fins da legislação, ao "espaço virtual interconectado por meio da internet, compreendendo redes mundiais de computadores, dispositivos móveis, plataformas digitais, sistemas de comunicação on-line e quaisquer outras tecnologias interativas que permitam a criação, o armazenamento, a transmissão e a recepção de dados e informações".

Além disso, o texto estabelece, no art. 2.2027-E, os seguintes fundamentos[1] da disciplina denominada "Direito Civil Digital":

> I – o respeito à privacidade, à proteção de dados pessoais e patrimoniais, bem como à autodeterminação informativa;
>
> II – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> III – a inviolabilidade da intimidade, da honra, da vida privada e da imagem da pessoa;

1 De acordo com o Parecer nº 1 da Subcomissão de Direito Digital, a justificativa para cada um dos fundamentos apresentados é delineada a seguir:

"I - Respeito à privacidade, proteção de dados pessoais e autodeterminação informativa: O avanço tecnológico tem gerado uma coleta massiva de dados pessoais, demandando a criação de medidas que assegurem a privacidade dos cidadãos. Garantir a autodeterminação informativa é crucial para empoderar os indivíduos sobre o uso de suas informações, promovendo transparência e confiança.

II - Liberdade de expressão, informação, comunicação e opinião: A liberdade de expressão é um pilar da democracia, essencial para o desenvolvimento de uma sociedade plural. A disciplina do direito digital deve promover um ambiente online onde a livre expressão de ideias seja protegida, respeitando limites éticos e legais.

III - Inviolabilidade da intimidade, honra e imagem: A proteção da intimidade, honra e imagem é vital para preservar a dignidade humana. O direito digital deve assegurar que as pessoas sejam resguardadas contra invasões indevidas, garantindo um ambiente digital que promova o respeito e a integridade.

IV - Desenvolvimento econômico e tecnológico e inovação: Fomentar o desenvolvimento econômico e tecnológico é essencial para a competitividade global. A disciplina do direito digital deve criar um ambiente regulatório que promova a inovação, estimulando o surgimento de novas tecnologias e a expansão de setores estratégicos.

V - Livre iniciativa, livre concorrência e defesa do consumidor: A proteção do ambiente digital deve abranger a promoção da livre iniciativa e concorrência, assegurando um mercado competitivo e transparente. Além disso, é imperativo garantir a defesa dos consumidores, protegendo-os contra práticas abusivas e assegurando a qualidade e segurança dos produtos e serviços digitais.

VI - Inclusão social e promoção da igualdade: O acesso equitativo às tecnologias digitais é fundamental para a inclusão social. A disciplina proposta busca criar condições para que todos os cidadãos possam usufruir dos benefícios do ambiente digital, reduzindo disparidades e promovendo a igualdade de oportunidades.

VII - Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais: A disciplina do direito digital deve ser orientada pelos princípios fundamentais dos direitos humanos, garantindo o livre desenvolvimento da personalidade, a dignidade e a plena participação dos indivíduos na sociedade digital, respeitando e promovendo sua cidadania".(Brasil, 2025)

IV – o desenvolvimento e a inovação econômicos, científicos e tecnológicos, assegurando a integridade e a privacidade mental, a liberdade cognitiva, o acesso justo, a proteção contra práticas discriminatórias e a transparência algorítmica;

V – a livre iniciativa e a livre concorrência;

VI – a inclusão social, promoção da igualdade e da acessibilidade digital; e

VII – o efetivo respeito aos direitos humanos, ao livre desenvolvimento da personalidade e dignidade das pessoas e o exercício da cidadania pelas pessoas naturais.

Elucida-se que "o direito civil digital preservará o pleno exercício da liberdade de informação, da liberdade de contratar, da liberdade contratual e do respeito à privacidade e à liberdade das pessoas, em harmoniosa relação com a regulação desses serviços" (art. 2027-F). São estabelecidos, ainda, no §1º do art. 2.027-F, os seguintes parâmetros fundamentais para a interpretação dos fatos, atos, negócios e atividades civis que ocorrerem no ambiente digital, que não excluem outros previstos no ordenamento jurídico pátrio, relacionados à matéria, ou nos tratados internacionais de que o Brasil seja signatário:

I – o respeito à dignidade humana de todas as pessoas;

II – o favorecimento à inclusão e à acessibilidade no ambiente digital, para a participação de todos, em igualdade de oportunidade e de condições, com acesso às tecnologias digitais;

III – a garantia da segurança do ambiente digital, revelada pelos sistemas de proteção de dados, capazes de preservar os usuários contra investidas que lhes coarctem o discernimento, ainda que momentaneamente;

IV – a promoção de conduta ética no ambiente digital, respeitando os direitos autorais, preservando a informação, sua segurança e correção, bem como a integridade de dados;

V – o combate à desigualdade digital;

VI – o respeito aos direitos e à proteção integral de crianças e de adolescentes também no ambiente digital.

No Capítulo II, que trata "Da pessoa no ambiente digital", está prevista uma série de direitos das pessoas, naturais ou jurídicas, no ambiente digital, sem prejuízo de outros previstos em lei ou em documentos e tratados dos quais o Brasil seja signatário, nos termos do art. 2.027-I, *caput*. Destacam-se, no contexto de exercício da autonomia privada, da preservação da dignidade e da segurança das pessoas no ambiente digital, os seguintes direitos:

I – o reconhecimento de sua identidade, presença e liberdade no ambiente digital;

II – a proteção de dados e informações pessoais, em consonância com a legislação de proteção de dados pessoais;

III – a garantia dos direitos de personalidade, em todas as suas expressões, como a de dignidade, de honra, de privacidade e de seu livre desenvolvimento;

III – a liberdade de expressão, de imprensa, de comunicação e de associação no ambiente digital;

IV – o acesso a mecanismos de justa composição e de reparação integral dos danos em casos de violação de direitos no ambiente digital;

V – outros direitos estabelecidos na legislação brasileira, aplicáveis ao ambiente digital.

O Capítulo III, por sua vez, trata das situações jurídicas no ambiente digital, previstas no art. 2.027-S. Essas correspondem às interações no ambiente digital de que resultem responsabilidade por vantagens ou desvantagens, direitos e deveres entre pessoas naturais, pessoas jurídicas ou entidades digitais, e que serão constituídas quando:

I – houver acordo de vontades manifestado, de forma expressa ou tácita, no ambiente digital;

II – houver acordo de vontades manifestado, de forma expressa ou tácita, envolvendo sujeito em ambiente analógico com máquina ou equipamento digital;

III – houver acordo que gere direitos e deveres reconhecíveis e exigíveis objetivamente;

IV – as partes envolvidas tiverem capacidade, legitimação e legitimidade para atuar no ambiente digital, conforme definido pela legislação aplicável, e quando de sua conduta nascer responsabilidade objetiva;

V – de algum fato objetivo derive para usuários e provedores vínculo que os obrigue a adotar conduta ou comportamento de que resulte responsabilidade para uma das partes.

Há, ainda, expressa indicação à observação ao diálogo das fontes normativas, conforme disposição do § 2º do art. 2027-S:

As situações jurídicas digitais estão submetidas, entre outras, às normas de direito contratual, direito do consumidor, direitos autorais, direitos de personalidade e de proteção de dados pessoais, à observância da boa-fé, da função social e da transparência, bem como às normas e termos de uso estabelecidos pelas plataformas e serviços digitais envolvidos, desde que não contrariem a legislação brasileira, sobretudo as normas cogentes ou de ordem pública.

Esse, portanto, é o contexto no qual se insere o Livro Direito Civil Digital. Passaremos à análise das temáticas selecionadas para esse estudo: a) Pessoa no ambiente digital: exclusão de dados pessoais, de informações e desindexação; b) Neurodireitos; c) Direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo; d) Patrimônio digital; e) Presença e identidade de crianças e adolescentes no ambiente digital; f) Inteligência artificial; g) Celebração de contratos por meios digitais; e h) Assinaturas eletrônicas.

ANÁLISES TEMÁTICAS

03

3 ANÁLISES TEMÁTICAS

3.1 Da pessoa no ambiente digital: exclusão de dados pessoais, de informações e desindexação

O texto abaixo está contido no Capítulo II do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Da pessoa no ambiente digital."

CAPÍTULO II

DA PESSOA NO AMBIENTE DIGITAL

Art. 2.027-J. À pessoa é possível requerer a exclusão de dados pessoais e de dados pessoais sensíveis expostos sem finalidade justificada, nos termos da lei.

§ 1º São suscetíveis de exclusão, nos termos do *caput*, além de outros, os dados:

I – pessoais que deixarem de ser necessários para a finalidade que motivou a sua coleta ou tratamento;

II – pessoais cujo consentimento que autorizou seu tratamento tenha sido retirado, ainda que autorizado por lei;

III – cujo tratamento foi ou veio a ser objeto de oposição por seu titular;

IV – pessoais tratados ilegalmente;

V – que devam ser eliminados ao término de seu tratamento;

VI – pessoais excessivamente expostos sem finalidade justificada

§ 2º O direito à exclusão de dados pessoais e de dados pessoais

sensíveis, de que cuida este artigo, não pode ser exercido enquanto seu tratamento ou divulgação:

I – forem relevantes ao exercício da liberdade de expressão;

II – forem manifestamente públicos;

III – decorrerem do cumprimento de dever legal;

IV – forem considerados excluídos do rol daqueles que a lei considera passíveis de exclusão.

Art. 2.027-K. A pessoa pode requerer a exclusão permanente de dados ou de informações a ela referentes, que representem lesão aos seus direitos de personalidade, diretamente no site de origem em que foi publicado.

Parágrafo único. Para os fins deste artigo, são requisitos para a concessão do pedido:

I – a demonstração de transcurso de lapso temporal razoável da publicação da informação verídica;

II – a ausência de interesse público ou histórico relativo à pessoa ou aos fatos correlatos;

III – a demonstração de que a manutenção da informação em sua fonte poderá gerar significativo potencial de dano à pessoa ou aos seus representantes;

IV – a demonstração de que a manutenção da informação em sua fonte poderá gerar significativo potencial de dano à pessoa ou aos seus representantes legítimos e nenhum benefício para quem quer que seja;

V – a presença de abuso de direito no exercício da liberdade de expressão e de informação;

VI – a concessão de autorização judicial.

§ 1º Se provado pela pessoa interessada que a informação veio ao conhecimento de quem levou seu conteúdo a público, por erro, dolo, coação, fraude ou por outra maneira ilícita, o juiz deverá imediatamente ordenar sua exclusão, invertendo-se o ônus da prova para que o site onde a informação se encontra indexada demonstre razão para sua manutenção.

§ 2º Consideram-se obtidos ilicitamente, entre outros, os dados e as informações que tiverem sido extraídos de processos judiciais que correm em segredo de justiça, os obtidos por meio de hackeamento ilícito, os que tenham sido fornecidos por comunicação pessoal, ou a respeito dos quais o divulgador tinha dever legal de mantê-los em sigilo.

Art. 2.027-L. À pessoa é possível requerer a aplicação do direito à desindexação, que consiste na remoção do link que direciona a busca para informações inadequadas, não mais relevantes, abusivas ou excessivamente prejudiciais ao requerente e que não possuem utilidade ou finalidade para a exposição, de mecanismos de busca, websites ou plataformas digitais, permanecendo o conteúdo no site de origem.

Parágrafo único. São hipóteses de remoção de conteúdo, entre outras, as que envolvem a exposição de:

I - imagens pessoais explícitas ou íntimas;

II – a pornografia falsa involuntária envolvendo o usuário;

III - informações de identificação pessoal dos resultados da pesquisa;

IV - conteúdo que envolva imagens de crianças e de adolescentes.

Art. 2.027-M. Os mecanismos de busca deverão estabelecer procedimentos claros e acessíveis para que os usuários possam solicitar a exclusão de seus dados pessoais ou daqueles que estão sob sua autoridade parental, tutela ou curatela.

Art. 2.027-N. É dever de todos os provedores e usuários do ambiente digital:

I - responder, de forma objetiva, segundo as disposições deste Código e de leis especiais, pelos danos que seus atos e atividades causarem a outras pessoas;

II - respeitar os direitos autorais e a propriedade intelectual;

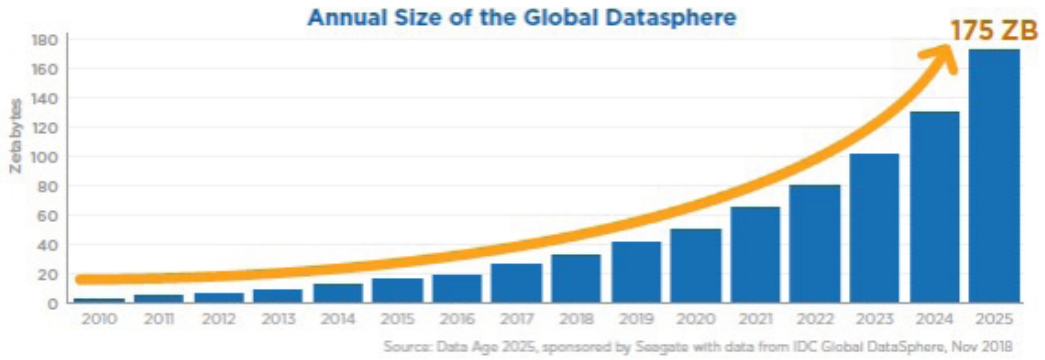
III - agir com ética e responsabilidade, evitando práticas que possam causar danos a outros usuários, aos provedores ou à integridade e à segurança do ambiente digital;

IV - observar as leis e os regulamentos aplicáveis às condutas e às transações realizadas no ambiente digital.

3.1.1 Abordagem teórica da temática

A quantidade de dados gerados, capturados e reproduzidos está em rápida expansão. São desde dados instantâneos, de pequena escala, *big data* ou informações em tempo real. O estudo Data Age 2025 (Seagate & IDC, 2018), realizado pela Seagate e pelo IDC, traz informações sobre crescimento da quantidade de dados armazenados com a estimativa de que chegaríamos em 2025 com 175 *zettabytes* de dados armazenados, como se verifica abaixo.

Figura 3 – Dados anuais sobre armazenamento de dados



Fonte: SEAGATE & IDC.

Atualmente, estamos inseridos em um contexto digital global que é comumente denominado de "sociedade informacional, global e em rede", conforme a denominação de Manuel Castells (2018). O autor afirma que alguns elementos caracterizam esse contexto: a) estabelecimento de uma sociedade em rede; b) descentralização tanto das fontes quanto dos destinos das informações; c) fluxo contínuo de retroalimentação de dados; d) desenvolvimento de uma ampla variedade de dispositivos tanto para processamento quanto para comunicação.

Verifica-se que, nesse cenário, a vida em rede possibilita a rápida disseminação de dados com o compartilhamento instantâneo de informações em escala global e o armazenamento duradouro dessas informações (Doneda, 2021). Nesse sentido, Byung-Chul Han (2018, p. 36) afirma que: "A mídia digital não oferece apenas uma janela para o assistir passivo, mas sim também portas através das quais passamos informações produzidas por nós mesmos."

O ambiente digital possibilitou que a informação seja tratada e apresentada como uma "mercadoria", revelando uma outra faceta da sociedade da informação. Stefano Rodotá (2008, p. 113) afirma que: "a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações." Segundo Laura Porto (2024a):

> A facilidade com que se publica e dissemina conteúdo online cria um arquivo virtual permanente, onde cada post, comentário ou notícia pode ser encontrado anos depois, perpetuando qualquer tipo de informações, sendo elas relevantes, verídicas, prejudiciais ou não.
>
> Essa eternização digital pode ter consequências profundas na vida das pessoas. Informações que poderiam ser temporárias ou esquecidas no mundo analógico permanecem acessíveis indefinidamente, impactando a reputação, a privacidade e até mesmo o bem-estar emocional dos indivíduos. No contexto atual, onde a presença online é uma extensão significativa da identidade pessoal, ter controle sobre o que permanece disponível é crucial.

Há uma relação entre a conectividade digital e a construção da identidade pessoal, pois, a partir de buscas on-line, é possível acessar eventos passados, permitindo que possam interferir negativamente no desenvolvimento pessoal e gerar instabilidade nas relações.

Nesse cenário, a distinção entre as esferas pública e privada é reconfigurada e transforma a concepção do direito à privacidade, que se expande, indo além do mero direito de ser deixado em paz ou do direito ao sigilo. Ele passa a abranger, de maneira mais significativa, o direito ao controle sobre as informações pessoais (Doneda, 2021). Segundo Rodotá (2008, p. 17), a privacidade vai além do eixo "pessoa-informação-segredo", para abarcar, também, o eixo "pessoa-informação-circulação-controle".

A ampliação da digitalização na vida cotidiana, com o uso massivo de dados pessoais no âmbito plataformas digitais, tornou imperiosa a criação de instrumentos que visem assegurar a autodeterminação informativa, a fim de proteger a privacidade, bem como preservar a identidade digital e garantir a dignidade dos usuários no ambiente virtual. Tais instrumentos permitem o controle sobre o fluxo de dados pessoais com a exclusão e a correção de eventuais dados incorretos.

Como explica Laura Schertel Ferreira Mendes (2020), o conceito de autodeterminação informativa tem origem na decisão de 1983 do Tribunal Constitucional Alemão, quando se analisou a constitucionalidade da Lei do Censo que permitia o fornecimento de dados pessoais com a possibilidade de cruzamento desses dados com outros registros públicos.

Diante da quantidade de dados disponíveis na internet, os serviços de busca possibilitam e facilitam a localização de informações. Dessa forma, a desindexação é uma ferramenta que possibilita que um conteúdo deixe de ser exibido, a partir de determinadas palavras-chave ou critérios de pesquisa, em resultados de busca por motores de pesquisa ou plataformas digitais. A desindexação não se confunde com apagamento de dados ou de conteúdo, já que as informações continuarão disponíveis no site de origem e a informação ainda poderá ser localizada com outros parâmetros. Já a exclusão de dados refere-se à remoção de conteúdo dos sites de origem ou das bases de dados.

Em síntese, segundo a distinção proposta por Luciano Floridi (2015), no contexto digital, a informação deve ser compreendida em dois planos distintos: o da sua disponibilidade (ou existência do conteúdo) e o da sua acessibilidade (ou facilidade de acesso, geralmente viabilizada por *links*). O direito à desindexação refere-se à retirada de links que direcionam a conteúdos considerados inadequados, desatualizados ou excessivos, especialmente quando sua exposição pública deixa de cumprir uma finalidade legítima. Essa remoção ocorre nos mecanismos de busca, sites ou plataformas digitais, sem que isso implique a exclusão do conteúdo na sua página original (Guardia, 2020).

É possível traçar a consolidação do direito à desindexação ao caso conhecido como González vs. Google España (Luz; Wachowicz, 2018), julgado pelo Tribunal de Justiça da União Europeia em 2014 (União Europeia, 2014). O caso envolveu Mario Costeja González, um advogado espanhol, cuja residência foi penhorada e leiloada em função de dívidas relacionadas à seguridade social da Espanha, o jornal La Vanguardia e o Google Espanha.

Em 1998, o jornal mencionado publicou, no site dedicado a leilões públicos, uma notícia sobre a venda de um apartamento relacionada a Mario Costeja González. Contudo, a venda não se concretizou, pois a dívida com a seguridade social foi quitada a tempo. Mesmo assim, a reportagem sobre a execução continuou a aparecer nos resultados de busca do Google. Em 2009, González solicitou ao jornal a remoção do seu nome das pesquisas, mas o pedido foi negado. No ano seguinte, ele fez a mesma solicitação ao Google Espanha, que também a rejeitou.

O autor recorreu à Agência Espanhola de Proteção de Dados, que determinou que o Google removesse os dados dos resultados de busca. O Google recorreu ao Tribunal de Justiça da União Europeia e, em 2014, o tribunal decidiu a favor de Mario Costeja González com base nos artigos 12º, alínea b, que trata do apagamento e bloqueio de dados, e 14º, alínea a, da Diretiva Europeia 95/46, que aborda o direito de oposição ao uso de informações pessoais. A decisão tornou-se um grande referencial jurisprudencial sobre a temática, pois trouxe elementos importantes para a definição e consolidação do direito ao esquecimento, bem como estabeleceu o reconhecimento do direito à desindexação em atendimento ao princípio da autodeterminação informativa.

A exclusão de dados ou informações e a desindexação estão relacionadas ao pleno desenvolvimento da personalidade e à capacidade de preservação e gerenciamento de informações pessoais, refletindo verdadeiramente o direito à autodeterminação informativa. Tais práticas atuam como um fator de tensão para a liberdade de expressão. A partir disso, há necessidade de estabelecer parâmetros claros para evitar usos abusivos que possam comprometer outros direitos, como o direito à memória, a liberdade de imprensa e o interesse público.

Nesse cenário, o papel das plataformas digitais também ganha relevância, já que operacionalizam esses direitos do ponto de vista técnico, tema que será aprofundado no item

a seguir. Além disso, do ponto de vista normativo, as suas políticas internas de moderação e gestão de dados impactam diretamente na gestão do conteúdo nas plataformas digitais. Desta forma, torna-se, portanto, essencial examinar como essas plataformas estruturam suas diretrizes, os critérios de avaliação de pedidos de remoção de dados e de desindexação, bem como os mecanismos de transparência e *accountability* implementados, como se verá a seguir.

3.1.2 O tratamento da matéria pelas plataformas digitais

a) Google

O Google (Google, 2024b; Youtube, 2025) informa que as políticas de conteúdo e produtos da Pesquisa Google são aplicáveis globalmente e estabelece políticas de conteúdo pessoal, de acordo com as seguintes categorias:

• Remover imagens pessoais explícitas ou íntimas dos resultados da pesquisa do Google;

• Remover imagens explícitas não consensuais e falsas dos resultados da pesquisa do Google;

• Remover a associação com conteúdo sexual irrelevante dos resultados da pesquisa do Google relacionados ao meu nome;

• Remover informações de identificação pessoal (PII) ou conteúdo de *doxing* dos resultados da pesquisa do Google;

• Remover informações sobre mim em sites com práticas abusivas de remoção de conteúdo dos resultados da pesquisa do Google;

• Conteúdo relacionado a indivíduos menores de 18 anos;

• Remover imagens de menores (não explícitas);

• Denunciar material de abuso sexual infantil (explícito);

• Se o proprietário do site tiver removido as informações, elas também serão removidas da Pesquisa Google como parte do nosso processo normal de atualização. No entanto, você também pode pedir a atualização de conteúdo usando a ferramenta adequada.

Esclarece, ainda, que, caso o conteúdo não se qualifique para a remoção de acordo com as políticas de conteúdo pessoal listadas acima, há outras opções disponibilizadas:

> Opções de remoção de conteúdo fora da Pesquisa Google
>
> O Google remove conteúdo dos resultados da pesquisa que viola nossas políticas de conteúdo e produtos. Se você quiser que algum conteúdo seja removido dos resultados da pesquisa, mas ele não viola nossas políticas, pode haver outras opções.

Remover conteúdo da página de origem

Em geral, a melhor opção é remover o conteúdo na página de origem.

Entrar em contato com o proprietário do site

Embora possamos impedir que determinado conteúdo apareça nos nossos resultados da pesquisa, não podemos removê-lo dos sites que o hospedam. O proprietário do site é responsável por ele. Para remover o conteúdo, a melhor opção é entrar em contato com o proprietário do site. Aprenda a entrar em contato com o proprietário de um site.

Remover conteúdo do seu próprio site

Se a imagem está no seu site, aprenda a bloquear seu conteúdo dos resultados da pesquisa do Google.

Remover conteúdo enviado para uma plataforma de mídias sociais

A maioria das plataformas de mídias sociais tem recursos de ajuda sobre as políticas de remoção de imagens, privacidade de conteúdo e processos de recuperação de conta. talvez ainda haja outras opções. Ou você pode consultar a Central de Ajuda Jurídica.

Acrescenta, ainda, que o conteúdo pode ser removido por motivos jurídicos específicos, incluindo, mas não se limitando à violação de direitos autorais, às violações da política contra pirataria ou ao mandado judicial. Além disso, caso haja algum conteúdo explícito envolvendo uma pessoa compartilhado sem a permissão dela, a plataforma disponibiliza os serviços de suporte.

b) Meta

A Meta apresenta uma política sobre "Pedido de remoção legal" (Meta, 2024a), conforme se verifica abaixo.

Se você acredita que um conteúdo no Instagram ou no Threads viola seus direitos legais pessoais ou a legislação local, é possível que ele também viole os Padrões da Comunidade da Meta (por exemplo, bullying, assédio ou conduta de ódio).

Para denunciar um conteúdo que você acredita que não segue os Padrões da Comunidade da Meta, use o link que aparece no menu suspenso ao lado do conteúdo. Você também pode denunciar um conteúdo na Central de Ajuda.

Se você estiver na UE e preferir enviar um pedido para remover um conteúdo que acredita ser ilegal, preencha nosso formulário de pedido de remoção legal.

Lembre-se: denunciar um conteúdo no Instagram ou no Threads não garante que ele será removido.

Caso haja violação de direitos de propriedade intelectual, a política é a seguinte:

Sobre propriedade intelectual

A Meta quer ajudar pessoas e organizações a proteger seus direitos de propriedade intelectual. A Meta não permite a publicação de conteúdo que viole os direitos de propriedade intelectual de terceiros, inclusive direitos autorais e de marca comercial.

Direitos autorais

Os direitos autorais são um direito legal que visa proteger obras originais de autoria (por exemplo, livros, músicas, filmes ou peças artísticas). Em geral, os direitos autorais protegem a expressão original da ideia, como palavras ou imagens. Eles não protegem fatos e ideias, mas podem proteger as palavras ou imagens originalmente usadas para expressar uma ideia. Os direitos autorais também não protegem nomes, títulos e slogans. No entanto, há outro direito legal chamado marca comercial que pode proteger esses itens. Saiba mais sobre como denunciar violações de direitos autorais:

Central de Ajuda do Facebook

Central de Ajuda do Instagram

Central de Ajuda do WhatsApp

Central de Ajuda do Meta Quest

Se você acredita que um conteúdo na Meta infringe seus direitos autorais, também pode denunciá-lo para nós por meio de uma das seguintes formas:

Formulário de denúncia de direitos autorais | Facebook

Formulário de denúncia de direitos autorais | Instagram

Formulário de propriedade intelectual | WhatsApp

Formulário de propriedade intelectual | Quest

Formulário de propriedade intelectual | Meta AI

Marca comercial

Uma marca comercial é uma palavra, um slogan, um símbolo ou um desenho (por exemplo, o nome ou o logotipo da marca) que distingue os produtos ou

serviços oferecidos por uma pessoa, grupo ou empresa daqueles oferecidos por outros. Em geral, a lei de marca comercial visa evitar que o consumidor se confunda quanto a quem fornece ou está associado a um produto ou serviço.

Saiba mais sobre como denunciar violações de marca comercial

Central de Ajuda do Facebook

Central de Ajuda do Instagram

Central de Ajuda do WhatsApp

Central de Ajuda do Meta Quest

Se você acredita que um conteúdo na Meta infringe seus direitos de marca comercial, também pode denunciá-lo para nós por meio de uma das seguintes formas:

Formulário de denúncia de marca comercial | Facebook

Formulário de denúncia de marca comercial | Instagram

Formulário de propriedade intelectual | WhatsApp

Formulário de propriedade intelectual | Quest

Formulário de propriedade intelectual | Meta AI

Apelação de remoção de conteúdo

Se removermos seu conteúdo devido a uma denúncia de propriedade intelectual, você receberá uma notificação da Meta. Essa notificação pode incluir o nome e o endereço de e-mail do detentor de direitos que fez a denúncia, bem como outros detalhes sobre a denúncia.

Se você acredita que seu conteúdo não deveria ter sido removido, você pode tentar resolver o problema ao entrar em contato diretamente com o detentor dos direitos. Você também tem a opção de enviar uma apelação. Nesse caso, você receberá instruções sobre como fazer isso na notificação enviada para você.

Política para infratores reincidentes de propriedade intelectual

Publicar repetidamente conteúdo que infrinja os direitos de propriedade intelectual de outra pessoa pode resultar em restrições adicionais. Sua conta ou perfil pode ser desabilitado, ou você pode enfrentar limitações na sua capacidade de postar conteúdo ou acessar determinados recursos e funcionalidades. (Meta, 2024b).

c) TikTok

O TikTok não adota uma política específica voltada à desindexação de conteúdos, mas prevê a possibilidade de remoção de conteúdos que violem uma série de diretrizes, incluindo infrações a direitos autorais, divulgação de informações pessoais, práticas de assédio, discurso de ódio, exploração sexual infantil, terrorismo, conteúdos relacionados à automutilação e ao suicídio, nudez não consensual e a publicação de *deepfakes* com potencial prejudicial. Sua atuação, nesse aspecto, limita-se à exclusão direta dos materiais de seu próprio ambiente digital, sem mecanismos próprios voltados à limitação da repercussão desses conteúdos em motores de busca externos (TikTok, 2024).

d) X (antigo Twitter)

O X (antigo Twitter) estabelece a possibilidade de remoção de conteúdos que: violem direitos autorais; divulguem de informações privadas de terceiros; sejam caracterizados como práticas de abuso e assédio, bem como de exploração sexual de menores; exponham conteúdos violentos ou com ameaças; veiculem *deepfakes* e discursos de ódio. Por outro lado, a plataforma não adota uma política voltada à desindexação de conteúdos, já que atua diretamente na exclusão direta do material considerado violador (X, 2024).

3.1.3 Experiências normativas do direito estrangeiro e transnacional

3.1.3.1 União Europeia

O direito à desindexação é um conceito importante na proteção de dados pessoais na União Europeia. Como visto anteriormente, foi estabelecido e ampliado pelo Tribunal de Justiça da União Europeia e está consagrado no Regulamento Geral de Proteção de Dados.

Os indivíduos podem solicitar aos motores de busca a remoção de links que direcionem para conteúdos que incluam os dados pessoais deles. Tais solicitações devem ser analisadas pelos motores de busca, que devem equilibrar os direitos de privacidade do indivíduo com o interesse público na informação. Em caso de negativa da solicitação, o indivíduo poderá recorrer às autoridades nacionais de proteção de dados nos Estados-Membros da UE.

No âmbito da União Europeia, o General Data Protection Regulation (União Europeia, 2016) prevê o direito ao apagamento de dados em seu artigo 17, nos seguintes termos:

> Artigo 17. Direito ao apagamento dos dados (direito a ser esquecido)
>
> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua coleta ou tratamento;

b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;

c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2;

d) Os dados pessoais foram tratados ilicitamente;

e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação legal decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;

f) Os dados pessoais foram coletados no contexto da oferta de serviços da sociedade da informação referidos no artigo 8.o, n.o 1.

2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado, nos termos do n.o 1, a apagar os dados pessoais, o responsável pelo tratamento, tendo em conta a tecnologia disponível e o custo de implementação, deve tomar medidas razoáveis, incluindo medidas técnicas, para informar os controladores que estão processando os dados pessoais de que o titular dos dados solicitou o apagamento por esses controladores de quaisquer links, ou cópia ou replicação desses dados pessoais.

3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:

a) Ao exercício da liberdade de expressão e de informação;

b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.o, n.o 2, alíneas h) e i), bem como do artigo 9.o, n.o 3;

d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, na medida em que o direito referido no n.o 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou

e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial. (Tradução nossa)

Além desse dispositivo, o artigo 21 prevê que:

> Direito de objeção
>
> 1 O titular dos dados terá o direito de se opor, por motivos relacionados à sua situação particular, a qualquer momento, ao processamento de dados pessoais que lhe digam respeito, com base na alínea (e) ou (f) do Artigo 6, incluindo a criação de perfis com base nessas disposições.
>
> O controlador não processará mais os dados pessoais, a menos que demonstre motivos legítimos e convincentes para o processamento que se sobreponham aos interesses, direitos e liberdades do titular dos dados ou para o estabelecimento, exercício ou defesa de reivindicações legais.
>
> 2. Quando dados pessoais forem processados para fins de marketing direto, o titular dos dados terá o direito de se opor a qualquer momento ao processamento de dados pessoais relativos a ele para tal marketing, o que inclui a criação de perfil na medida em que esteja relacionado a tal marketing direto.
>
> 3. Caso o titular dos dados se oponha ao processamento para fins de marketing direto, os dados pessoais não serão mais processados para tais fins.
>
> 4. No momento da primeira comunicação com o titular dos dados, o direito referido nos parágrafos 1 e 2 deve ser explicitamente levado ao conhecimento do titular dos dados e deve ser apresentado de forma clara e separada de qualquer outra informação.
>
> 5. No contexto da utilização de serviços da sociedade da informação, e não obstante a Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados que utilizem especificações técnicas.
>
> 6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do Artigo 89, o titular dos dados, por motivos relacionados com a sua situação particular, terá o direito de se opor ao tratamento dos dados pessoais que lhe digam respeito, a menos que o tratamento seja necessário para o desempenho de uma tarefa realizada por razões de interesse público.(Tradução nossa)

3.1.3.2 Reino Unido

No Reino Unido, o Data Protection Act (2018), que internalizou o GDPR europeu, assegura o direito ao apagamento de dados pessoais, incluindo a possibilidade de desindexação:[2]

2 No original:

"(1)The controller must erase personal data without undue delay where—

(a)the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or

(b)the controller has a legal obligation to erase the data.

Direito ao apagamento ou à restrição do tratamento

(1) O controlador deve apagar os dados pessoais sem demora injustificada quando:

(a) o tratamento dos dados pessoais violar as disposições da seção 35, dos parágrafos (1) a (3) da seção 36, ou das seções 37, 38(1), 39(1), 40, 41 ou 42; ou

(b) o controlador tiver a obrigação legal de apagar os dados.

(2) Quando o controlador for obrigado a apagar os dados pessoais nos termos do parágrafo (1), mas os dados precisarem ser mantidos para fins probatórios, o controlador deve, em vez de apagá-los, restringir o seu tratamento.

(3) Quando o titular dos dados contestar a exatidão dos dados pessoais, seja por meio de um pedido com base neste artigo, no artigo 46 ou de qualquer outra forma, mas não for possível verificar se os dados são ou não exatos, o controlador deve restringir o seu tratamento.

(4) O titular dos dados pode solicitar ao controlador o apagamento dos dados pessoais ou a restrição do seu tratamento, mas os deveres do controlador previstos neste artigo aplicam-se independentemente da formulação de tal pedido. (Reino Unido, 2018) (Tradução nossa).

Apesar da previsão expressa, a exclusão é ponderada frente à liberdade de expressão, ao interesse público e à prática jornalística.

3.1.3.3 Argentina

A Ley 25.326/2000 – Protección de los datos personales (Argentina, 2000) prevê que o titular dos dados tem o direito de solicitar a retirada ou o bloqueio total ou parcial de suas informações pessoais quando elas forem incorretas, inexatas, desatualizadas ou incompletas. A desindexação não é prevista na norma, mas já vem sendo reconhecida na jurisprudência local.

3.1.3.4 Chile

A Ley 19.628/1999 – Sobre protección de la vida privada (Chile,1999) prevê que o titular dos dados poderá solicitar a qualquer momento a eliminação ou cancelamento de seus dados pessoais quando eles não forem exatos ou estiverem desatualizados. Porém, a desindexação não é expressamente regulada.

(2)Where the controller would be required to erase personal data under subsection (1) but the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.

(3)Where a data subject contests the accuracy of personal data (whether in making a request under this section or section 46 or in any other way), but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.

(4)A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller under this section apply whether or not such a request is made)."

3.1.3.5 Síntese analítica das experiências normativas do direito estrangeiro e transnacional

Os direitos à exclusão de dados e à desindexação são uma concretização do direito à autodeterminação informativa e vêm sendo tratados com diferentes abordagens regulatórias pelos países. A experiências normativas que merece destaque é da União Europeia, com o Regulamento Geral de Proteção de Dados (GDPR) que reconhece, no artigo 17, de forma expressa, o chamado direito ao apagamento de dados. O Projeto de Lei nº 4, de 2025, está mais alinhado com a tradição europeia e busca estruturar um Direito Civil Digital com preocupação na tutela da personalidade e da autodeterminação informativa.

3.1.4 Estudos de caso

3.1.4.1 Brasil: Caso da Chacina da Candelária – Recurso Especial nº 1.334.097

Em 1993, no Rio de Janeiro, oito jovens em situação de rua, com idades entre 11 e 19 anos, foram assassinados diante da Igreja da Candelária enquanto dormiam, sem poder se defender. Um dos sobreviventes conseguiu identificar que os autores do crime eram policiais militares. Três policiais foram condenados, enquanto outros três foram absolvidos.

Em 2006, a Rede Globo exibiu a reconstituição dos fatos relacionados ao caso no programa "Linha Direta", o que culminou no ajuizamento de ação de indenização por danos morais. Embora a 3ª Vara Cível do Rio de Janeiro tenha julgado improcedente o pedido, a decisão foi posteriormente reformada pelo TJRJ, em sede de apelação, reconhecendo a responsabilidade da emissora pela violação de direitos da parte autora.

A Rede Globo recorreu da decisão ao STJ, argumentando que não havia violado a privacidade do autor, uma vez que os acontecimentos retratados eram de domínio público e a reconstituição realizada estava adstrita aos fatos do caso. O Tribunal, contudo, negou provimento ao recurso, tendo decidido de maneira unânime que pela condenação da emissora deveria ao pagamento de indenização por danos morais, devido à ofensa à honra do autor, com fundamento no direito ao esquecimento. O relator do processo, ministro Luis Felipe Salomão, integrante da 4ª Turma, reconheceu que:

> 2 [...] o cerne da controvérsia passa pela ausência de contemporaneidade da notícia de fatos passados, que reabriu antigas feridas já superadas pelo autor e reacendeu a desconfiança da sociedade quanto à sua índole. O autor busca a proclamação do seu direito ao esquecimento, um direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado.
>
> [...]
>
> 9. Não há dúvida de que a história da sociedade é patrimônio imaterial do povo e nela se inserem os mais variados acontecimentos e personagens ca-

pazes de revelar, para o futuro, os traços políticos, sociais ou culturais de determinada época. Todavia, a historicidade da notícia jornalística, em se tratando de jornalismo policial, há de ser vista com cautela. Há, de fato, crimes históricos e criminosos famosos; mas também há crimes e criminosos que se tornaram artificialmente históricos e famosos, obra da exploração midiática exacerbada e de um populismo penal satisfativo dos prazeres primários das multidões, que simplifica o fenômeno criminal às estigmatizadas figuras do "bandido" vs. "cidadão de bem".

10. É que a historicidade de determinados crimes por vezes é edificada à custa de vários desvios de legalidade, por isso não deve constituir óbice em si intransponível ao reconhecimento de direitos como o vindicado nos presentes autos. Na verdade, a permissão ampla e irrestrita a que um crime e as pessoas nele envolvidas sejam retratados indefinidamente no tempo – a pretexto da historicidade do fato – pode significar permissão de um segundo abuso à dignidade humana, simplesmente porque o primeiro já fora cometido no passado. Por isso, nesses casos, o reconhecimento do "direito ao esquecimento" pode significar um corretivo – tardio, mas possível – das vicissitudes do passado, seja de inquéritos policiais ou processos judiciais pirotécnicos e injustos, seja da exploração populista da mídia.

[....]

14. Se os condenados que já cumpriram a pena têm direito ao sigilo da folha de antecedentes, assim também a exclusão dos registros da condenação no Instituto de Identificação, por maiores e melhores razões aqueles que foram absolvidos não podem permanecer com esse estigma, conferindo-lhes a lei o mesmo direito de serem esquecidos.

[...]

18. No caso concreto, a despeito de a Chacina da Candelária ter se tornado – com muita razão – um fato histórico, que expôs as chagas do País ao mundo, tornando-se símbolo da precária proteção estatal conferida aos direitos humanos da criança e do adolescente em situação de risco, o certo é que a fatídica história seria bem contada e de forma fidedigna sem que para isso a imagem e o nome do autor precisassem ser expostos em rede nacional. Nem a liberdade de imprensa seria tolhida, nem a honra do autor seria maculada, caso se ocultassem o nome e a fisionomia do recorrido, ponderação de valores que, no caso, seria a melhor solução ao conflito. (Superior Tribunal de Justiça, 2013a)

3.1.4.2 Brasil: Caso Aída Curi – Recurso Especial nº 1.335.153

O homicídio de Aída Curi, ocorrido em 1958, foi objeto de uma reportagem realizada pela Rede Globo anos após o homicídio, em 2004. Diante da veiculação dessa reportagem, os familiares de Aída Curi ajuizaram ação indenizatória em face da emissora de televisão, alegando que a reportagem teria causado constrangimento e exposição aos parentes da vítima e que o fato ocorrido não pertence mais ao domínio público.

Os pedidos foram julgados improcedentes em 1º e 2º graus no Tribunal de Justiça do Estado do Rio de Janeiro. Em sede de Recurso Especial, o relator do acórdão, ministro Luis Felipe Salomão afirmou que a reportagem focou mais nos fatos do que na vítima e ressaltou que o crime sempre esteve associado ao nome da vítima e, por isso, foi divulgado dessa forma. Ele também concluiu que a imagem da falecida não foi usada de maneira degradante ou desrespeitosa. Além disso, destacou que, com o tempo, a dor e os constrangimentos enfrentados pelos familiares vão diminuindo, tornando o impacto da divulgação do crime menos intenso, como se verifica na ementa do acórdão:

> RECURSO ESPECIAL. DIREITO CIVIL-CONSTITUCIONAL. LIBERDADE DE IMPRENSA VS. DIREITOS DA PERSONALIDADE. LITÍGIO DE SOLUÇÃO TRANSVERSAL. COMPETÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA. DOCUMENTÁRIO EXIBIDO EM REDE NACIONAL. LINHA DIRETA-JUSTIÇA. HOMICÍDIO DE REPERCUSSÃO NACIONAL OCORRIDO NO ANO DE 1958. CASO "AIDA CURI". VEICULAÇÃO, MEIO SÉCULO DEPOIS DO FATO, DO NOME E IMAGEM DA VÍTIMA. NÃO CONSENTIMENTO DOS FAMILIARES. DIREITO AO ESQUECIMENTO. ACOLHIMENTO. NÃO APLICAÇÃO NO CASO CONCRETO. RECONHECIMENTO DA HISTORICIDADE DO FATO PELAS INSTÂNCIAS ORDINÁRIAS. IMPOSSIBILIDADE DE DESVINCULAÇÃO DO NOME DA VÍTIMA. ADEMAIS, INEXISTÊNCIA, NO CASO CONCRETO, DE DANO MORAL INDENIZÁVEL. VIOLAÇÃO AO DIREITO DE IMAGEM. SÚMULA N. 403/STJ. NÃO INCIDÊNCIA.
>
> [...]
>
> 2. Nos presentes autos, o cerne da controvérsia passa pela ausência de contemporaneidade da notícia de fatos passados, a qual, segundo o entendimento dos autores, reabriu antigas feridas já superadas quanto à morte de sua irmã, Aida Curi, no distante ano de 1958. Buscam a proclamação do seu direito ao esquecimento, de não ter revivida, contra a vontade deles, a dor antes experimentada por ocasião da morte de Aida Curi, assim também pela publicidade conferida ao caso décadas passadas.
>
> 3. Assim como os condenados que cumpriram pena e os absolvidos que se envolveram em processo-crime (REsp. n. 1.334/097/RJ), as vítimas de crimes e seus familiares têm direito ao esquecimento – se assim desejarem –, direito esse consistente em não se submeterem a desnecessárias lembranças de fatos passados que lhes causaram, por si, inesquecíveis feridas. Caso contrário, che-

gar-se-ia à antipática e desumana solução de reconhecer esse direito ao ofensor (que está relacionado com sua ressocialização) e retirá-lo dos ofendidos, permitindo que os canais de informação se enriqueçam mediante a indefinida exploração das desgraças privadas pelas quais passaram.

4. Não obstante isso, assim como o direito ao esquecimento do ofensor – condenado e já penalizado – deve ser ponderado pela questão da historicidade do fato narrado, assim também o direito dos ofendidos deve observar esse mesmo parâmetro. Em um crime de repercussão nacional, a vítima – por torpeza do destino – frequentemente se torna elemento indissociável do delito, circunstância que, na generalidade das vezes, inviabiliza a narrativa do crime caso se pretenda omitir a figura do ofendido.

5. Com efeito, o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, acontecimento que entrou para o domínio público, de modo que se tornaria impraticável a atividade da imprensa para o desiderato de retratar o caso Aida Curi, sem Aida Curi.

6. É evidente ser possível, caso a caso, a ponderação acerca de como o crime tornou-se histórico, podendo o julgador reconhecer que, desde sempre, o que houve foi uma exacerbada exploração midiática, e permitir novamente essa exploração significaria conformar-se com um segundo abuso só porque o primeiro já ocorrera. Porém, no caso em exame, não ficou reconhecida essa artificiosidade ou o abuso antecedente na cobertura do crime, inserindo-se, portanto, nas exceções decorrentes da ampla publicidade a que podem se sujeitar alguns delitos.

7. Não fosse por isso, o reconhecimento, em tese, de um direito de esquecimento não conduz necessariamente ao dever de indenizar. Em matéria de responsabilidade civil, a violação de direitos encontra-se na seara da ilicitude, cuja existência não dispensa também a ocorrência de dano, com nexo causal, para chegar-se, finalmente, ao dever de indenizar. No caso de familiares de vítimas de crimes passados, que só querem esquecer a dor pela qual passaram em determinado momento da vida, há uma infeliz constatação: na medida em que o tempo passa e vai se adquirindo um "direito ao esquecimento", na contramão, a dor vai diminuindo, de modo que, relembrar o fato trágico da vida, a depender do tempo transcorrido, embora possa gerar desconforto, não causa o mesmo abalo de antes.

8. A reportagem contra a qual se insurgiram os autores foi ao ar 50 (cinquenta) anos depois da morte de Aida Curi, circunstância da qual se conclui não ter havido abalo moral apto a gerar responsabilidade civil. Nesse particular, fazendo-se a indispensável ponderação de valores, o acolhimento do direito ao esquecimento, no caso, com a consequente indenização, consubstancia desproporcional corte à liberdade de imprensa, se comparado ao desconforto gerado pela lembrança. (Superior Tribunal de Justiça, 2013b)

3.1.4.3 Brasil: Casos Orkut (Recurso Extraordinário nº 1.057.258) e Facebook (Recurso Extraordinário nº 1.037.396)

Destacam-se, ainda, os recursos extraordinários nº 1.057.258 e nº 1.037.396, que correspondem, respectivamente, aos Temas de Repercussão Geral 533 e 987, recentemente julgados pelo Supremo Tribunal Federal.

O primeiro caso envolve a extinta rede social Orkut, gerida pelo Google, tendo como origem pedido formulado por professora do ensino médio para a exclusão de uma comunidade ofensiva, intitulada "Eu odeio a Aliandra", criada em 2009 – portanto, antes da vigência do Marco Civil da Internet. O Orkut recusou a remoção da página sem ordem judicial, o que levou ao Judiciário a reconhecê-lo como responsável civilmente pelos danos. Em sede recursal, porém, o Google sustenta que tal interpretação impõe um dever de censura prévia e afronta a liberdade de manifestação de seus usuários. Em suma, o RE nº 1.057.258 trata da possibilidade de responsabilização dos provedores por danos decorrentes de conteúdos ilícitos divulgados por usuários, especialmente quando não adotam providências a partir de notificações extrajudiciais.

Já o segundo caso teve origem em uma decisão da 2ª Turma do Colégio Recursal de Piracicaba (SP), a qual ordenou a exclusão de um perfil falso criado no Facebook, além do fornecimento de dados do terminal usado e fixou indenização por danos morais. A Meta (empresa detentora do Facebook) alegou que as obrigações de remoção sem decisão judicial prévia violariam a liberdade de expressão e também representariam risco de censura. No RE 1.037.396, portanto, foi discutida a constitucionalidade do art. 19 do Marco Civil da Internet, que condiciona a responsabilidade civil dos provedores ao descumprimento de ordem judicial específica.

Em síntese, os dois recursos suscitaram o exame da compatibilidade entre o regime de responsabilidade civil previsto no art. 19 do Marco Civil da Internet e os princípios constitucionais da liberdade de expressão, do devido processo legal e da proteção da honra e da imagem. Os Temas de Repercussão Geral 533 e 987 serão analisados com maior profundidade no item 3.3 deste estudo, dedicado especificamente à responsabilidade das plataformas digitais.

3.1.5 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

Em síntese, tanto a exclusão de dados quanto a desindexação representam instrumentos centrais no esforço de adaptação do ordenamento jurídico brasileiro aos desafios impostos pela era digital. Como se verá a seguir, a Emenda Constitucional nº 115/2022 alçou a proteção de dados pessoais à categoria de direito fundamental autônomo (inciso LXXIX do art. 5º da Constituição Federal). Além disso, o Marco Civil da Internet e a Lei Geral de Proteção de Dados constituem um sistema de proteção de dados pessoais e fundamentam o direito à exclusão de dados e à desindexação.

Porém, o projeto de lei da reforma do Código Civil traz elementos e critérios claros para o exercício desses direitos, que serão avaliados judicialmente com o objetivo de balizar os direitos à privacidade e à informação, de forma a manter íntegra a informação pública quando necessária, como veremos no próximo item.

3.1.5.1 Exclusão de dados pessoais e de informações

A Lei Geral de Proteção de Dados contempla o direito à autodeterminação informativa no art. 2º, inciso II, além do respeito à privacidade (inciso I); a liberdade de expressão, de informação, de comunicação e de opinião (inciso III); a inviolabilidade da intimidade, da honra e da imagem (inciso IV); o desenvolvimento econômico e tecnológico e a inovação (inciso V); a livre iniciativa, a livre concorrência e a defesa do consumidor (inciso VI) e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (inciso VII). Além disso, como já visto, o direito à proteção de dados pessoais, com fundamento na autodeterminação informativa, foi alçado à categoria de direito autônomo com status de direito fundamental por meio da Emenda Constitucional nº 155 [3], que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A LGPD estabelece, no art. 7º, as bases legais para o tratamento de dados pessoais, e, no art. 11, os requisitos específicos aplicáveis ao tratamento de dados pessoais sensíveis:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I – mediante o fornecimento de consentimento pelo titular;
>
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V – quando necessário para a execução de contrato ou de procedimentos

3 Nos termos da EC nº 115:

"Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:'

Art. 5º (...) LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

(...)

Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:

"Art. 21. (...) XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei."

Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

"Art. 22. (...) XXX – proteção e tratamento de dados pessoais.

(...).'

preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Já o art. 18 da LGPD prevê que, a qualquer momento e mediante solicitação, o titular dos dados pessoais tem o direito de obter do controlador informações relacionadas aos dados que estão sendo processados, incluindo:

> I- confirmação da existência de tratamento;
>
> II – acesso aos dados;
>
> III – correção de dados incompletos, inexatos ou desatualizados;
>
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
>
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

A LGPD prevê ainda as hipóteses de término do tratamento de dados pessoais (art. 15), bem como a possibilidade de eliminação dos dados pessoais (art. 16):

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II – fim do período de tratamento;
>
> III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.
>
> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I – cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

> IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A LGPD, portanto, prevê, de forma expressa, o direito à eliminação de dados pessoais. Tais dados devem ser tratados com fundamento em bases legais que refletem o reconhecimento normativo da importância da autodeterminação informativa e da preservação da privacidade. Embora a LGPD não discipline de maneira específica a desindexação, também não nega a possibilidade de sua concretização. O Projeto de Lei nº 4, de 2025, traz maior sistematicidade e densidade normativa a essas temáticas, incorporando dispositivos voltados à tutela da personalidade na esfera digital e admitindo a possibilidade de desindexação e de remoção de conteúdos. Além disso, ao abordar temas como a transparência algorítmica e o gerenciamento da presença digital, o projeto trata dos efeitos da indexação algorítmica.

O Marco Civil da Internet, por sua vez, garante ao usuário o poder de requerer a exclusão definitiva dos dados pessoais que forneceu a uma aplicação de internet ao término da relação entre as partes, salvo nas situações em que a legislação exige a conservação desses registros, como previsto tanto nessa lei quanto na legislação sobre proteção de dados pessoais:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> [...]
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

O Superior Tribunal de Justiça (STJ), ao interpretar esse dispositivo, esclareceu que esse direito se limita aos dados inseridos voluntariamente pelo próprio usuário na plataforma (AgInt no RESP nº 1.593.873/SP, julgado em nov. 2016). Nos termos do Acórdão:

> Com relação aos provedores de aplicações de internet, a exclusão de dados pessoais configura-se como um direito subjetivo, que pode ser exercido sem qualquer condicionamento, salvo nos casos de guarda obrigatória de registros.
>
> Contudo, uma consideração importante deve ser feita. As aplicações de internet são definidas pelo Marco Civil da Internet como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". Assim, o direito à exclusão mencionado restringe-se às informações que o próprio indivíduo houver fornecido ao respectivo provedor de aplicações de internet. (Superior Tribunal de Justiça, 2016)

3.1.5.2 Desindexação

Como elucidado anteriormente, o direito à desindexação refere-se à retirada de links que direcionam a conteúdos considerados inadequados, desatualizados ou excessivos, especialmente quando sua exposição pública deixa de cumprir uma finalidade legítima. Essa remoção ocorre nos mecanismos de busca, sites ou plataformas digitais, sem que isso implique a exclusão do conteúdo na sua página original. Nesse cenário, restringir a acessibilidade – por exemplo, por meio da desindexação – pode ser uma medida eficaz para proteger a esfera privada do indivíduo, pois, ao reduzir drasticamente a visibilidade de determinado conteúdo nos resultados de busca, o seu impacto prático na circulação da informação é significativamente diminuído.

O tema, inclusive, já foi objeto de análise do Superior Tribunal de Justiça (STJ, 2018). Em 2018, ao julgar o Recurso Especial nº 1.660.168/RJ, o Tribunal consolidou o entendimento de que, em situações excepcionais, os direitos à intimidade, ao esquecimento e à proteção de dados pessoais podem prevalecer sobre o direito à informação, "a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca".

O caso teve origem em uma ação de obrigação de fazer, ajuizada por uma Promotora de Justiça que solicitava a desindexação, nos resultados de diferentes ferramentas de busca, de notícias que a vinculavam a suspeitas de fraude em concurso da Magistratura do Estado do Rio de Janeiro. A autora argumentava que a exposição contínua dessas notícias, ao serem acessíveis por meio de seu nome, causava danos à sua dignidade e privacidade e, por isso, requereu a filtragem dos resultados de busca que remetessem às reportagens em questão O juiz de primeira instância julgou improcedente o pedido, entendendo que os mecanismos de busca não seriam responsáveis pelo conteúdo das páginas indexadas. No entanto, após interposição de recurso, o Tribunal de Justiça do Rio de Janeiro reformou a decisão, estipulando que os provedores removessem os resultados que mencionassem seu envolvimento nas alegações de fraude. Diante disso, os provedores recorreram ao STJ por meio de Recurso Especial, o qual foi parcialmente provido apenas para reduzir o valor da multa diária fixada na decisão anterior, mantendo a decisão de desindexação dos links indicados.

Reconheceu-se, assim, o direito à desindexação como medida adequada à proteção da dignidade da pessoa humana e da privacidade, sem que isso implicasse exclusão do conteúdo original, conforme registrado no acórdão:

> No caso concreto, passado mais de uma década desde o fato noticiado, ao se informar como critério de busca exclusivo o nome da parte recorrente, o primeiro resultado apresentado permanecia apontando link de notícia de seu possível envolvimento em fato desabonador, não comprovado, a despeito da existência de outras tantas informações posteriores a seu respeito disponíveis na rede mundial.

3.1.5.3 Da responsabilidade por violação aos direitos à exclusão de dados e à desindexação

A LGPD trata da responsabilidade pelo descumprimento das obrigações relativas à proteção de dados pessoais em seus artigos 42 e seguintes. O art. 42 estabelece que tanto o controlador quanto o operador de dados são responsáveis pela reparação de danos – sejam eles patrimoniais, morais, individuais ou coletivos – causados em decorrência de atividades de tratamento de dados pessoais que violem a legislação de proteção de dados:

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

Além disso, o juiz pode determinar a inversão do ônus da prova em favor do titular dos dados quando verificar a plausibilidade da alegação – nos termos do artigo 300 do CPC combinado com o §2º do art. 42 da LGPD –, especialmente nos casos em que fique demonstrada a hipossuficiência do titular para produzir provas ou quando a produção dessas provas lhe for excessivamente onerosa.

Importante esclarecer que a LGPD considera ilícito o tratamento de dados que não atenda às suas determinações, sujeitando os responsáveis às consequências civis daí decorrentes. O art. 44 da LGPD é particularmente claro ao afirmar que o tratamento será irregular sempre que não garantir o nível de segurança que o titular razoavelmente pode esperar. Nesse sentido, o dispositivo enumera três critérios que devem orientar a

avaliação da regularidade do tratamento: (i) o modo como o tratamento é realizado; (ii) os resultados e os riscos previsíveis dessa atividade; e (iii) as tecnologias disponíveis à época em que o tratamento ocorreu.

A obrigação de adotar medidas adequadas de segurança e de preservar a integridade dos dados também é reforçada pelo parágrafo único do art. 44 da LGPD, que institui um regime de responsabilidade aplicável ao controlador e ao operador que descumprirem as exigências de segurança previstas no art. 46 da lei[4]. Tal responsabilidade é universal, alcançando todos os agentes de tratamento, sejam eles públicos ou privados. Isso inclui o Poder Judiciário e os prestadores de serviços que realizam operações de tratamento de dados para a Justiça, os quais respondem por eventuais danos causados por falhas na segurança das informações sob sua guarda. No caso de a administração pública figurar como controladora, os prestadores de serviços poderão ser acionados regressivamente. Já nas relações de direito privado, a responsabilidade entre os agentes de tratamento é solidária.

Finalmente, o art. 43 da LGPD delimita as hipóteses em que os agentes de tratamento podem se eximir de responsabilidade: (i) quando demonstrarem que não realizaram o tratamento de dados que lhes foi atribuído; (ii) quando, embora tenham realizado o tratamento, provarem que não houve violação à legislação de proteção de dados; ou (iii) quando o dano decorrer exclusivamente de culpa do próprio titular dos dados ou de terceiro.

No que tange à responsabilidade dos provedores, o Marco Civil da Internet prevê, no art. 18, que o provedor de serviços de internet não poderá ser responsabilizado civilmente por danos resultantes de conteúdo criado por terceiros. Porém, nos termos do art. 19, caso haja ordem judicial específica para remoção de conteúdo gerado por terceiros e o provedor de serviços de internet não tomar as providências para tornar indisponível o conteúdo apontado como infringente, este poderá ser responsabilizado civilmente:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

4 "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Outra hipótese de responsabilidade subsidiária está prevista no art. 21 do Marco Civil da Internet:

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

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

O tema da responsabilidade dos provedores será analisado com maior profundidade no tópico 3.3, que trata da regulação das plataformas digitais e da moderação de conteúdo no âmbito do direito ao ambiente digital transparente e seguro.

3.1.6 Comentários sobre o texto do projeto da reforma do Código Civil

O Capítulo II, do Livro Direito Civil Digital, intitulado "Da pessoa no ambiente digital", prevê a possibilidade de a pessoa requerer a exclusão de dados pessoais e de dados

pessoais sensíveis, expostos sem finalidade justificada, nos termos de seu art. 2.027-J. O texto prevê que são suscetíveis de exclusão, além de outros, os dados:

a) pessoais que deixarem de ser necessários para a finalidade que motivou a sua coleta ou tratamento (§ 1º, I);

b) pessoais cujo consentimento que autorizou seu tratamento tenha sido retirado, ainda que autorizado por lei (§ 1º, II);

c) cujo tratamento foi ou veio a ser objeto de oposição por seu titular (§ 1º, III);

d) pessoais tratados ilegalmente (§ 1º, IV);

e) que devam ser eliminados ao término de seu tratamento (§ 1º, V);

f) pessoais excessivamente expostos sem finalidade justificada (§ 1º, VI).

Além disso, o direito à exclusão de dados pessoais e de dados pessoais sensíveis não pode ser exercido enquanto o tratamento ou a divulgação dele:

a) forem relevantes ao exercício da liberdade de expressão (§ 2º, I);

b) forem manifestamente públicos (§ 2º, II);

c) decorrerem do cumprimento de dever legal (§ 2º, III);

d) forem considerados excluídos do rol daqueles que a lei considera passíveis de exclusão (§ 2º, IV).

Estabelece, ainda, que a pessoa pode requerer a exclusão permanente de dados ou de informações a ela referentes, que representem lesão aos seus direitos de personalidade, diretamente no site de origem em que foi publicado (art. 2.027-K). Os seguintes requisitos devem ser observados para a realização do pedido:

a) a demonstração de transcurso de lapso temporal razoável da publicação da informação verídica (inciso I);

b) a ausência de interesse público ou histórico relativo à pessoa ou aos fatos correlatos (inciso II);

c) a demonstração de que a manutenção da informação em sua fonte poderá gerar significativo potencial de dano à pessoa ou aos seus representantes (inciso III);

d) demonstração de que a manutenção da informação em sua fonte poderá gerar significativo potencial de dano à pessoa ou aos seus representantes legítimos e nenhum benefício para quem quer que seja (inciso IV);

e) a presença de abuso de direito no exercício da liberdade de expressão e de informação (inciso V);

f) a concessão de autorização judicial (inciso VI).

Caso haja a comprovação de que o conteúdo foi publicado por erro, dolo, coação, fraude ou por outra maneira ilícita, o juiz deverá imediatamente ordenar a exclusão dessa,

com a inversão do ônus da prova para que o site no qual a informação se encontra indexada demonstre razão para a manutenção (art. 2.027-K, §1º).

O texto do projeto de lei caracteriza como ilícitos os dados e as informações extraídos de processos judiciais que correm em segredo de justiça, bem como os obtidos por meio de hackeamento ilícito, tenham sido fornecidos por comunicação pessoal, ou a respeito dos quais o divulgador tinha dever legal de mantê-los em sigilo. Segundo Laura Porto:

> O direito à exclusão de informações surge como uma resposta necessária para equilibrar o acesso à informação e a proteção dos direitos de personalidade. Este direito reconhece que, embora a liberdade de expressão e o direito à informação sejam pilares fundamentais da democracia, eles devem ser ponderados com a necessidade de proteger a privacidade individual. Ao permitir que as pessoas solicitem a remoção definitiva de dados prejudiciais, a lei oferece uma ferramenta essencial para garantir que todos possam reconstituir suas vidas sem o fardo constante de um passado perpetuado digitalmente. (Porto, 2024a)

Verifica-se que o texto prevê claras delimitações para o instituto, que só serão aplicáveis no caso de informações pessoais que: a) deixarem de ser necessárias para a finalidade que motivou a sua coleta ou o seu tratamento; b) cujo consentimento que autorizou o seu tratamento tenha sido retirado, ainda que autorizado por lei; c) cujo tratamento foi ou veio a ser objeto de oposição por seu titular; d) pessoais tratados ilegalmente; e) que devam ser eliminados ao término de seu tratamento; f) excessivamente expostos sem finalidade justificada.

Além disso, afasta do âmbito de aplicação o tratamento ou a divulgação de dados pessoais de interesse público que tratem de fatos históricos e se enquadrarem nas seguintes hipóteses: a) forem relevantes ao exercício da liberdade de expressão; b) forem manifestamente públicos; c) decorrerem do cumprimento de dever legal; d) forem considerados excluídos do rol daqueles que a lei considera passíveis de exclusão.

Em relação ao Tema 786, "Aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares", a proposta da exclusão de dados ou informações, prevista no texto da reforma, não conflita com o tema, pois o STF entendeu que "eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais — especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral — e as expressas e específicas previsões legais nos âmbitos penal e cível" (Supremo Tribunal Federal, 2021).

Embora não haja um direito ao esquecimento pela simples passagem do tempo, o STF decidiu que deverá haver a análise do caso concreto para verificar se há abuso ou excesso da disponibilização da informação. Nesse sentido, o projeto de lei traz critérios, requisitos e condicionantes para o exercício do direito de exclusão de dados ou informações.

Sobre a questão da veiculação de fatos notórios, Laura Porto, ao analisar os casos Aída Curi e da Chacina da Candelária, que foram objeto de detalhamento neste estudo, afirma que:

> Os casos relatados, tratam de fatos notórios, que possuem um relevante interesse social, pois são eventos que marcaram a história de seus respectivos países e têm um grande interesse público. No entanto, a questão aqui se dá quando não temos este apelo envolvido, mas sim um ponto pessoal sobre a vida de alguém, que pode ser eu ou você, e essa pessoa simplesmente não quer aquela informação exposta.
>
> A questão toma forma quando informações privadas e pessoais, sem relevância pública significativa, continuam a ser acessíveis na internet. Esse tipo de exposição pode ser profundamente prejudicial para o indivíduo envolvido. Fato é que hoje a internet nos traz uma pena "perpétua" de qualquer situação que envolva o nosso nome. Mais do que uma condenação no âmbito penal, onde se
>
> paga a dívida com a sociedade através de penas estipuladas pelo Estado e, uma vez cumpridas, se está livre, a permanência dessas informações online perpetua o conteúdo.
>
> Entramos então em uma discussão sobre a proteção dos direitos de personalidade frente à nova realidade digital em que nos encontramos. A manutenção de informações privadas e pessoais na internet, sem relevância pública significativa, pode causar danos emocionais e sociais irreparáveis. Indivíduos podem enfrentar diversas questões como estigmatização e discriminação, devido à perpetuação de informações antigas que não refletem mais sua realidade atual. A exposição contínua a esses dados infringe o direito fundamental à privacidade, dignidade e livre desenvolvimento, criando uma forma de punição perpétua que excede qualquer sentença judicial. (Porto, 2024a)

O projeto de lei traz também, neste capítulo, o direito à desindexação, prevendo a possibilidade de "remoção do link que direciona a busca para informações inadequadas, não mais relevantes, abusivas ou excessivamente prejudiciais ao requerente e que não possuem utilidade ou finalidade para a exposição, de mecanismos de busca, *websites* ou plataformas digitais, permanecendo o conteúdo no site de origem" (art. 2.027-L). São hipóteses previstas para a remoção do conteúdo, porém, aquelas que envolvem a exposição de:

a) imagens pessoais explícitas ou íntimas (inciso I);

b) pornografia falsa involuntária envolvendo o usuário (inciso II);

c) informações de identificação pessoal dos resultados da pesquisa (inciso III);

d) conteúdo que envolva imagens de crianças e de adolescentes (inciso IV).

Estabelece também, nos termos do art. 2.027-M, a necessidade de previsão de procedimentos claros e acessíveis pelas plataformas de mecanismos de buscas para que os usuários possam solicitar a exclusão de seus dados pessoais ou daqueles que estão sob a sua autoridade parental, tutela ou curatela.

Há, ainda, conforme art. 2.027-N, a previsão de que provedores de serviços e usuários respondam objetivamente, conforme estabelecido pelo Código e pela legislação específica, pelos prejuízos ocasionados a terceiros em decorrência de suas ações e atividades, bem como devem respeitar os direitos autorais e a propriedade intelectual; agir com ética e responsabilidade, evitando práticas que possam causar danos a outros usuários, aos provedores ou à integridade e à segurança do ambiente digital; atender rigorosamente às normas e regulamentações pertinentes às práticas e transações efetuadas no ambiente digital.

Como se verifica, o Capítulo II do Projeto de Lei nº 4, de 2025, introduz avanços significativos na tutela da pessoa no ambiente digital, buscando construir um equilíbrio entre a proteção dos direitos da personalidade e os novos desafios da circulação massiva de dados pessoais na sociedade informacional. Em suma, o projeto confere unidade e densidade normativa a conceitos que vinham sendo desenvolvidos apenas de forma doutrinária ou jurisprudencial.

Um dos pontos de maior inovação do projeto reside na positivação do direito à desindexação, inspirado no entendimento do Tribunal de Justiça da União Europeia no emblemático caso *Google Spain v. Costeja González*, além do fortalecimento da proteção jurídica em relação à exclusão de dados pessoais e sensíveis, à gestão da presença digital e ao direito à eliminação de conteúdos excessivos ou desproporcionais. Ademais, o projeto prevê, de modo explícito, critérios objetivos para o exercício do direito à exclusão, superando a fragmentação hoje existente entre a LGPD, o Marco Civil da Internet e decisões jurisprudenciais isoladas. Outro significativo aspecto inovador é a previsão de procedimentos claros e acessíveis, a serem implementados pelas plataformas digitais e mecanismos de busca, para que os usuários possam exercer seus direitos de forma efetiva e célere.

3.2 Da pessoa no ambiente digital: neurodireitos

O texto abaixo está contido no Capítulo II do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Da pessoa no ambiente digital".

CAPÍTULO II

DA PESSOA NO AMBIENTE DIGITAL

Art. 2.027-O. Os neurodireitos são parte indissociável da personalidade e recebem a mesma proteção desta, não podendo ser transmitidos, renunciados ou limitados.

§ 1º São considerados neurodireitos as proteções que visam

preservar a privacidade mental, a identidade pessoal, o livre arbítrio, o acesso justo à ampliação ou melhoria cerebral, a integridade mental e a proteção contra vieses, das pessoas naturais, a partir da utilização de neurotecnologias.

§ 2º São garantidos a toda pessoa natural os seguintes neurodireitos:

I – direito à liberdade cognitiva, vedado o uso de neurotecnologias de forma coercitiva ou sem consentimento;

II – direito à privacidade mental, concebido como direito de proteção contra o acesso não autorizado ou não desejado a dados cerebrais, vedada a venda ou transferência comercial;

III – direito à integridade mental, entendido com o direito à não manipulação da atividade mental por neurotecnologias, vedada a alteração ou eliminação do controle sobre o próprio comportamento sem consentimento;

IV – direito de continuidade da identidade pessoal e da vida mental, com a proteção contra alterações na identidade pessoal ou coerência de comportamento, vedadas alterações não autorizadas no cérebro ou nas atividades cerebrais;

V – direito ao acesso equitativo a tecnologias de aprimoramento ou extensão das capacidades cognitivas, segundo os princípios da justiça e da equidade;

VI – direito à proteção contra práticas discriminatórias, enviesadas a partir de dados cerebrais.

§ 3º Os neurodireitos e o uso ou acesso a dados cerebrais poderão ser regulados por normas específicas, desde que preservadas as proteções e as garantias conferidas aos direitos de personalidade.

3.2.1 Abordagem teórica da temática

O campo da neurociência, encarregado de aprofundar o estudo acerca do sistema nervoso humano e das emoções, tem se expandido cada vez mais nos últimos anos. Esse ramo do conhecimento é composto por cinco áreas de estudo específicas: neurociência cognitiva, neuropsicologia, neurociência comportamental, neurofisiologia e neuroanatomia (Lima, 2024a).

Com os avanços da neurociência e das neurotecnologias, surgiram dispositivos capazes de modificar a atividade cerebral e captar os sinais elétricos originados no sistema nervoso (Rodrigues, 2024). A partir de 1990, na "Década do Cérebro" (Ventura, 2010), o ambiente clínico e médico foi transformado pelo aperfeiçoamento do estudo acerca do funcionamento do cérebro e da mente humanos, principalmente no controle neural das funções motoras, sensoriais e vegetativas, dos comportamentos e mecanismos, como fala, locomoção, memória, atenção, conhecimento, sentimentos, entre outros relacionados à fisiologia humana.

A neurociência tem contribuído para elucidar o funcionamento das doenças neurológicas e mentais por intermédio da compreensão do sistema nervoso patológico. Doenças como Parkinson, autismo, paralisia cerebral, depressão e ansiedade, entre outras patologias que causam sofrimento e incapacidade, além de representarem custos econômicos elevados, são exemplos de patologias que alcançaram níveis notáveis de reconhecimento e evolução científicos e tecnológicos ao longo das últimas décadas.

Semelhante ao que ocorre com a inteligência artificial, a neurotecnologia é considerada uma área tecnológica estratégica e, por isso, é alvo de robustos investimentos por parte de vários países. O progresso dos estudos na área da neurociência possibilitou cenários otimistas – antes presenciados apenas em filmes de ficção científica –, visto que a interface cérebro-máquina, hoje, não é só uma realidade, mas também um propósito.

Nesse cenário, importa destacar que a inteligência artificial está sendo integrada ao desenvolvimento das neurotecnologias a fim de usar protótipos computacionais com o objetivo de replicar as funções fisiológicas integradas com o sistema nervoso. A partir da fusão e modulação cérebro-máquina, empresas privadas, como a Neuralink, prometem recuperar funções relacionadas à locomoção de pacientes com lesões na medula espinhal, por meio de chip implantado na região cerebral (G1, 2024).

O uso de neurotecnologias, particularmente no campo das Interfaces Cérebro-Computador (BCIs, na sigla em inglês), está se tornando cada vez mais palpável e importante. As BCIs possibilitam a comunicação direta entre o cérebro humano e os dispositivos tecnológicos, permitindo uma vasta gama de aplicações em áreas como saúde, reabilitação, entretenimento e até mesmo aprimoramento cognitivo (Porto, 2024c).

Nesse contexto, é possível observar a ascensão de possibilidades de intervenção no sistema neural. O funcionamento desses dispositivos está relacionado à atividade elétrica neuronal. Logo, os chips cerebrais são utilizados para recolher a atividade elétrica realizada pelos neurônios ao se comunicarem uns com os outros. Eles podem ser inseridos de forma invasiva, ou seja, diretamente no córtex cerebral, ou de forma não invasiva, quando são inseridos na superfície da cabeça, como um eletroencefalograma. Essa atividade neural é captada pelos eletrodos e submetida a um processador, que interpreta esses sinais e, graças a tecnologias como a IA, é possível traduzir os sinais recebidos em comandos especiais.

Porém, há uma apreensão acerca dos limites das influências que essas aplicações podem ter sobre o livre-arbítrio. Considera-se, por exemplo, a possibilidade de que tais dispositivos possam influenciar o estado emocional de uma pessoa, induzindo felicidade, tristeza ou até mesmo impulsionando-a a cometer atos ilícitos. Dado que a extensão dessas influências não é plenamente compreendida, torna-se fundamental estabelecer diretrizes regulatórias para o assunto. Nesse sentido, Laura Porto (2024c) sustenta que:

> Embora as neurotecnologias ofereçam inúmeros benefícios e promessas de avanços significativos em várias áreas da vida humana, também é importante reconhecer os ônus e os riscos associados. Entre esses desafios estão questões relacionadas à privacidade e segurança dos dados neurais, potenciais usos indevidos ou manipulativos das informações cerebrais, bem como preocupações éticas sobre o consentimento informado e a autonomia individual. Além disso, o surgimento de desigualdades sociais e econômicas no acesso e na utilização das neurotecnologias também é uma preocupação legítima.

A tecnologia de implantes cerebrais gera grande controvérsia, especialmente no que se refere à proteção dos direitos fundamentais devido ao seu potencial de falha na privacidade dos dados, o que levanta inúmeras preocupações éticas.

O termo "neurodireitos" foi introduzido em 2017 pelos pesquisadores Ienca e Andorno (2017), que evidenciaram as limitações do sistema internacional de direitos humanos para os desafios das tecnologias neurocientíficas. Yuste, Goering e Arcas afirmam que:

> Muitas das recomendações sobre neurotecnologia refletem a necessidade de pesquisadores da indústria e da academia assumirem as responsabilidades inerentes ao desenvolvimento de dispositivos e sistemas que podem causar transformações profundas. Eles podem recorrer a estruturas já existentes para promover a inovação responsável.
>
> Por exemplo, o *UK Engineering and Physical Sciences Research Council* fornece um quadro para incentivar inovadores a "antecipar, refletir, envolver-se e agir" de maneiras que "promovam oportunidades socialmente desejáveis para a ciência e inovação, realizadas no interesse público". Na área da IA, a IEEE *Standards Association* lançou uma iniciativa global de ética em 2016 para integrar a ética ao design de processos de IA e sistemas autônomos.
>
> Historicamente, a busca por lucro muitas vezes supera a responsabilidade social no mundo corporativo, e, mesmo que individualmente os tecnólogos busquem beneficiar a humanidade, podem enfrentar dilemas éticos complexos para os quais não estão preparados. Acreditamos que a mentalidade poderia ser transformada e os produtores de dispositivos mais bem equipados ao integrar um código de ética nas indústrias e academias.
>
> Um primeiro passo seria incluir treinamentos de ética para engenheiros, desenvolvedores e pesquisadores acadêmicos ao ingressarem em empresas ou laboratórios. Esses profissionais poderiam ser ensinados a refletir mais pro-

> fundamente sobre como seus avanços podem contribuir positivamente para a sociedade, em vez de fragmentá-la.
>
> Essa abordagem é semelhante à usada na medicina. Estudantes de medicina aprendem sobre a confidencialidade do paciente, o princípio de não causar dano e seus deveres de beneficência e justiça, e são obrigados a seguir o Juramento de Hipócrates para manter os mais altos padrões da profissão.
>
> Os benefícios clínicos e sociais das neurotecnologias são imensos, mas, para aproveitá-los, é essencial orientar seu desenvolvimento de forma a respeitar, proteger e fortalecer o que há de melhor na humanidade. (Tradução nossa)[5] (Yuste, Goering e Arcas, 2017)

Em contrapartida ao avanço da neurotecnologia, surgem questões no que diz respeito ao direito ao livre arbítrio, à identidade pessoal, à privacidade mental, ao acesso igualitário às neurotecnologias e à proteção contra vieses. Com isso, há a necessidade de tutelar juridicamente os bens da vida afetados por tal avanço. Desse modo, tem-se a gênese dos neurodireitos como arcabouço jurídico, com o fito de proteger e preservar o cérebro e a mente humanos.

Os neurodireitos são divididos em cinco tipos, conforme a *Neurorights Foundation* (2023): os direitos à privacidade mental, à identidade pessoal, ao livre arbítrio, ao acesso justo à ampliação mental e a proteção contra vieses.

Diante da insuficiência do tratamento da matéria em nível nacional e internacional, é essencial a implementação de normativas que garantam a proteção em todas as etapas de desenvolvimento e de uso das neurotecnologias. Como aponta Laura Porto:

> Em última análise, a regulamentação é essencial para preservar a dignidade humana, a integridade mental e a liberdade individual em um mundo cada vez mais permeado pela tecnologia. É hora de reconhecer e proteger os neurodi-

5 No original: "Underlying many of these recommendations is a call for industry and academic researchers to take on the responsibilities that come with devising devices and systems capable of bringing such change. In doing so, they could draw on frameworks that have already been developed for responsible innovation. In addition to the guidelines mentioned above, the UK Engineering and Physical Sciences Research Council, for instance, provides a framework to encourage innovators to "anticipate, reflect, engage and act" in ways that "promote ... opportunities for science and innovation that are socially desirable and undertaken in the public interest". Among the various efforts to address this in AI, the IEEE Standards Association created a global ethics initiative in April 2016, with the aim of embedding ethics into the design of processes for all AI and autonomous systems. History indicates that profit hunting will often trump social responsibility in the corporate world. And even if, at an individual level, most technologists set out to benefit humanity, they can come up against complex ethical dilemmas for which they aren't prepared. We think that mindsets could be altered and the producers of devices better equipped by embedding an ethical code of conduct into industry and academia. A first step towards this would be to expose engineers, other tech developers and academic-research trainees to ethics as part of their standard training on joining a company or laboratory. Employees could be taught to think more deeply about how to pursue advances and deploy strategies that are likely to contribute constructively to society, rather than to fracture it. This type of approach would essentially follow that used in medicine. Medical students are taught about patient confidentiality, non-harm and their duties of beneficence and justice, and are required to take the Hippocratic Oath to adhere to the highest standards of the profession. The possible clinical and societal benefits of neurotechnologies are vast. To reap them, we must guide their development in a way that respects, protects and enables what is best in humanity."

> reitos como parte integrante dos direitos humanos universais, garantindo que todos possam se beneficiar dos avanços da neurociência e da tecnologia de maneira justa, equitativa e ética. (Porto, 2024c)

Diante desse cenário, o avanço das neurotecnologias impõe ao Direito contemporâneo o desafio de repensar as categorias tradicionais dos direitos da personalidade, a partir de uma nova camada relacionada à personalidade informacional e mental, com a salvaguarda da identidade digital e da esfera cognitiva.

Os neurodados, ao serem extraídos da atividade cerebral, possuem uma natureza qualitativamente distinta por refletirem, em tempo real, pensamentos, padrões mentais, emoções e processos decisórios. Portanto, a sua manipulação não apenas agrava riscos informacionais, mas inaugura possibilidades de interferência profunda na autodeterminação do indivíduo.

3.2.2 Experiências normativas do direito estrangeiro e transnacional

3.2.2.1 Organização para a Cooperação e Desenvolvimento Econômico (OCDE)

A Recomendação sobre Inovação Responsável em Neurotecnologia, adotada pelo Conselho da OCDE em 11 de dezembro de 2019 (OCDE, 2019), reconhece o potencial das neurotecnologias para melhorar a saúde e o bem-estar, bem como destaca os desafios éticos, legais e sociais associados a elas, estabelecendo nove princípios, que objetivam: a) promover a inovação responsável; b) priorizar a avaliação de segurança; c) promover a inclusão; d) fomentar a colaboração científica; e) permitir a deliberação social; f) fortalecer a capacidade de órgãos de supervisão e consultivos; g) proteger dados cerebrais pessoais e outras informações; h) promover culturas de responsabilidade e confiança entre os setores público e privado; i) antecipar e monitorar o uso e/ou abuso potencial não intencionado.

Entre as principais recomendações, podemos destacar: a) promoção da inovação responsável, com o incentivo à pesquisa e ao desenvolvimento de neurotecnologias de maneira responsável, considerando os impactos sociais e éticos; b) garantia da proteção dos direitos humanos e do desenvolvimento e do uso de tecnologias que respeitem os direitos humanos e as liberdades fundamentais; c) proteção de dados cerebrais pessoais e de outras informações obtidas por meio de neurotecnologia.

3.2.2.2 Organização dos Estados Americanos (OEA)

A "Declaração do Comitê Jurídico Interamericano sobre Neurociência, Neurotecnologias e Direitos Humanos: Novos Desafios Legais para as Américas" (OEA, 2021) é um documento adotado durante a 99ª Sessão do Comitê Jurídico Interamericano, realizada de 2 a 11 de agosto de 2021, com o objetivo de abordar os desafios legais emergentes decorrentes dos avanços em neurociência e neurotecnologias no contexto dos direitos humanos nas Américas.

Posteriormente, foi aprovada a "Declaração de Princípios Interamericanos em Matéria de Neurociências, Neurotecnologias e Direitos Humanos do Comitê Jurídico Interamericano", na 102ª Sessão Ordinária da OEA de 6 a 10 de março de 2023 (OEA, 2023), que prevê os seguintes princípios:

> Princípio 1: Preservação da identidade, autonomia e privacidade da atividade neural.
>
> Princípio 2: Proteção dos direitos humanos no design de neurotecnologias.
>
> Princípio 3: Compreensão de dados neurais como dados pessoais sensíveis.
>
> Princípio 4: Garantia de consentimento expresso e informado em relação aos dados neurais.
>
> Princípio 5: Promoção da igualdade, não discriminação e acesso equitativo às neurotecnologias.
>
> Princípio 6: Aplicação terapêutica exclusiva em relação à melhoria das capacidades cognitivas, evitando aumentar a desigualdade social.
>
> Princípio 7: Proteção da integridade neurocognitiva.
>
> Princípio 8: Governança transparente das neurotecnologias.
>
> Princípio 9: Supervisão e controle das neurotecnologias.
>
> Princípio 10: Acesso à proteção efetiva e a medidas reparadoras associadas ao desenvolvimento e uso de neurotecnologias.

A referida declaração estimula os Estados a criarem regulamentos e políticas que equilibrem a promoção da inovação com a proteção dos direitos humanos, assegurando que os avanços tecnológicos tragam benefícios à sociedade de maneira justa e ética.

3.2.2.3 Chile

A Lei nº 21.383/2021 alterou a Constituição chilena e incluiu a proteção dos neurodireitos no seu art. 19, 1º, que prevê:

> Art. 19. A Constituição assegura a todas as pessoas:
>
> 1°. O direito à vida e à integridade física e psíquica da pessoa.
>
> [...]
>
> O desenvolvimento científico e tecnológico estará a serviço das pessoas e será realizado com respeito à vida e à integridade física e psíquica. A lei regulará os requisitos, condições e restrições para sua utilização em pessoas, devendo especialmente resguardar a atividade cerebral, bem como as informações provenientes dela. (Tradução nossa). (Chile, 2021)[6]

6 No original: "Art. 19. La Constitución asegura a todas las personas:1º.- El derecho a la vida y a la integridad física y psíquica de la persona. [...]El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella;"

3.2.2.4 Espanha

A Espanha reconheceu a importância da regulamentação das neurotecnologias com a Carta de Derechos Digitales, que tem o objetivo de ser um guia regulatório nas proteções individual e coletiva no cenário digital. O Capítulo XXIV, intitulado "Direitos digitais no uso das neurotecnologias", prevê:

> 1. As condições, os limites e as garantias de implantação e uso das neurotecnologias nas pessoas poderão ser regulados por lei com a finalidade de:
>
> a) Garantir o controle de cada pessoa sobre sua própria identidade.
>
> b) Garantir a autodeterminação individual, soberania e liberdade na tomada de decisões.
>
> c) Assegurar a confidencialidade e segurança dos dados obtidos ou relativos aos seus processos cerebrais e o pleno domínio e disposição sobre os mesmos.
>
> d) Regular o uso de interfaces pessoa-máquina suscetíveis de afetar a integridade física ou psíquica.
>
> e) Assegurar que as decisões e processos baseados em neurotecnologias não sejam condicionados pelo fornecimento de dados, programas ou informações incompletas, indesejadas, desconhecidas ou tendenciosas ou por intromissões nas conexões neuronais.
>
> 2. Para garantir a dignidade da pessoa, a igualdade e a não discriminação, e de acordo, quando for o caso, com os tratados e convenções internacionais, a lei poderá regular situações e condições de uso das neurotecnologias que, além de sua aplicação terapêutica, visem o aumento cognitivo ou a estimulação ou potencialização das capacidades das pessoas. (Tradução nossa).(Espanha, 2021)[7]

7 No original: "XXVI - Derechos digitales en el empleo de las neurotecnologías:

1. Las condiciones, límites y garantías de implantación y empleo en las personas de las neurotec- nologías podrán ser reguladas por la ley con la finalidad de:

a) Garantizar el control de cada persona sobre su propia identidad.

b) Garantizar la autodeterminación individual, soberanía y libertad en la toma de decisiones.

c) Asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos.

d) Regular el uso de interfaces persona-máquina susceptibles de afectar a la integridad física o psíquica.

e) Asegurar que las decisiones y procesos basados en neurotecnologías no sean condicio- nadas por el suministro de datos, programas o informaciones incompletos, no deseados, desconocidos o sesgados.

2. Para garantizar la dignidad de la persona, la igualdad y la no discriminación, y de acuerdo en su caso con los tratados y convenios internacionales, la ley podrá regular aquellos supuestos y condi-

ciones de empleo de las neurotecnologías que, más allá de su aplicación terapéutica, pretendan el aumento cognitivo o la estimulación o potenciación de las capacidades de las personas."

3.2.2.5 França

A França, com a *Charte de Développement Responsable des Neurotechnologies* (França, 2022), estabeleceu princípios e diretrizes para proteger os neurodireitos no contexto do desenvolvimento e uso de neurotecnologias. Trata-se de um documento elaborado por atores públicos e privados, sem caráter vinculativo. Dessa forma, reflete o engajamento dos signatários de implementar a recomendação da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre o desenvolvimento responsável da inovação em neurotecnologias, a qual constitui a primeira norma internacional nesse domínio. Uma recomendação da OCDE é um instrumento jurídico não vinculativo, mas considerado compromissório.

Nesse sentido, os signatários da carta reconhecem o direito de preservar a identidade humana, a liberdade de pensamento, a autonomia, a liberdade cognitiva, a privacidade mental, o direito de se opor a qualquer uso não consentido ou abusivo dos dados cerebrais pessoais e de recusar qualquer manipulação não consentida ou abusiva de seu cérebro, nos seguintes termos:

> 1) Proteger os dados cerebrais pessoais, comprometendo-se a:
>
> a) Disponibilizar para os pacientes e usuários informações claras, acessíveis e rigorosas sobre a coleta, o tratamento e o uso dos dados cerebrais pessoais, bem como sobre o armazenamento, a difusão e o compartilhamento desses dados. O compartilhamento necessário para atender às exigências da ciência aberta será feito apenas com dados totalmente anonimizados, tomando todas as medidas razoavelmente praticáveis para prevenir uma reidentificação maliciosa;
>
> b) Reconhecer ao paciente e usuário o direito de recusar o compartilhamento dos dados cerebrais pessoais deles e melhorar a qualidade das informações e condições de consentimento, previamente à coleta dos dados;
>
> c) Utilizar todos os meios disponíveis para apagar ou modificar, mediante simples solicitação, os dados cerebrais pessoais coletados, exceto os já utilizados para fins de pesquisa, anonimizados e compartilhados com a comunidade científica;
>
> 2) Assegurar a confiabilidade, segurança e proteção dos dispositivos médicos e não médicos, comprometendo-se a:
>
> a) Garantir o uso de todos os meios disponíveis para proteger os dispositivos contra intrusões externas;
>
> b) Demonstrar, fora dos estudos clínicos, a eficácia dos dispositivos, produtos e serviços das aplicações não médicas propostas;
>
> c) Utilizar todos os meios disponíveis para garantir a reversibilidade dos dispositivos implantáveis e evitar efeitos remanescentes indesejáveis.
>
> d) Solicitar e considerar as reações e comentários dos pacientes e usuários;
>
> 3) Desenvolver uma comunicação ética e deontológica, comprometendo-se a:

a) Fazer todo o possível para evitar criar expectativas irreais ou, ao contrário, medos infundados em relação às neurotecnologias;

b) Fornecer, aos usuários de dispositivos comerciais, as evidências científicas dos benefícios e riscos esperados;

c) Garantir a transparência sobre o uso dos algoritmos, até mesmo sobre o conteúdo;

4) Prevenir os usos abusivos, as aplicações e as manipulações mal-intencionadas, comprometendo-se a:

a) Opor-se a aplicações que resultem em vigilância intrusiva, avaliação de uma pessoa sem consentimento prévio, manipulação abusiva do estado ou funcionamento cerebral, das funções cognitivas ou dos comportamentos de um sujeito, paciente ou usuário;

b) Abster-se de desenvolver e implementar aplicações e usos de neurotecnologias, caso sejam suscetíveis de prejudicar a pessoa humana;

c) Antecipar e impedir atividades que visem influenciar os processos decisórios de indivíduos ou grupos, limitando voluntariamente a liberdade e autodeterminação;

5) Levar em consideração as expectativas sociais, comprometendo-se a:

a) Questionar, na fase de concepção, o conceito de reflexividade, que convida a responder às necessidades reais da sociedade, e o conceito de inclusividade, que não limita o foco de uma atividade à simples relação produtor-consumidor;

b) Exercer uma vigilância particular para detectar aplicações que possam levar a discriminações e comunicar os meios empregados para evitá-las;

c) Participar, na medida do possível, do diálogo social;

d) Assegurar a acessibilidade do maior número possível de pessoas aos produtos e serviços desenvolvidos;

e) Reconhecer, na fase de concepção, a necessidade de antecipar os abusos potenciais e aplicar os procedimentos de "*ethics by design*" sempre que possível;

e f) Favorecer o desenvolvimento das neurotecnologias, especialmente no domínio da saúde mental. (Tradução nossa)[8]

3.2.2.6 Síntese analítica das experiências normativas do direito estrangeiro e transnacional

O debate sobre neurodireitos tem ganhado repercussão com experiências normativas relevantes, embora ainda muito centradas em iniciativas de *soft law*. Sem dúvida, a grande inovação foi realizada pelo Chile ao constitucionalizar o tema (Lei nº 21.383), vinculando o desenvolvimento neurotecnológico à proteção da integridade física e psíquica, com previsão de legislação específica para regulamentação.

8 A íntegra do texto está disponível no link: https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2023-01/charte-de-d-veloppement-responsable-des-neurotechnologies-25237.pdf

No âmbito da *soft law*, podemos destacar as experiências da Espanha, com a Carta de Direitos Digitais; da França, por meio da *Charte de Développement Responsable des Neurotechnologies;* da OCDE, com a Recomendação de 2019 e da OEA, com a Declaração do *Comitê Jurídico Interamericano sobre Neurociência, Neurotecnologias e Direitos Humanos: Novos Desafios Legais para as Américas*.

O Projeto de Lei nº 4, de 2025, aproxima-se do modelo chileno, reconhecendo expressamente os neurodireitos como dimensões da personalidade e avança ao definir garantias como liberdade cognitiva, privacidade mental, integridade mental, identidade pessoal, acesso equitativo a tecnologias de aprimoramento e proteção contra discriminações baseadas em dados cerebrais.

3.2.3 Estudos de caso

Embora ainda seja limitada a quantidade de casos expressamente rotulados como envolvendo "neurodireitos", observa-se o surgimento de decisões judiciais que, direta ou indiretamente, já enfrentam aspectos centrais dessa nova categoria de proteção da personalidade, com decisões relacionadas à tutela de dados sensíveis ampliados, abrangendo não apenas dados biométricos e genéticos, mas também informações oriundas de aplicações forenses de neurociência. Exemplificativamente, em países que vêm se destacando na positivação pioneira dos neurodireitos, como o Chile, já há decisão que reconhece, de maneira inaugural, a necessidade de proteção jurídica específica para os neurodados e para a integridade psíquica frente às novas tecnologias de interface cérebro-máquina.

3.2.3.1 Índia

No julgamento do caso *Smt. Selvi & Others vs. State of Karnataka* (Apelação Criminal nº 1267 de 2004), a Suprema Corte da Índia discutiu a compatibilidade constitucional do uso compulsório de determinadas técnicas de investigação criminal – entre elas, a narcoanálise, o teste do polígrafo e o chamado Perfil de Ativação Elétrica Cerebral (BEAP). A decisão ocorreu em face de uma série de recursos interpostos em ações penais que questionavam a legalidade da submissão de acusados, suspeitos ou testemunhas a esses procedimentos sem o seu consentimento. A Corte, ao examinar a matéria, concluiu que a imposição forçada desses métodos viola direitos fundamentais assegurados nos artigos 20(3) e 21 da Constituição indiana, firmando, assim, o entendimento de que tais exames apenas podem ser realizados mediante consentimento livre, esclarecido e voluntário da pessoa envolvida, sob pena de afronta à integridade mental, à privacidade e às garantias do devido processo legal.

3.2.3.2 Chile

Em 2023, a Corte Constitucional chilena julgou um caso envolvendo neurodireitos e proferiu uma importante decisão no caso Guido Girardi vs. Emotiv Inc. (Chile, 2023). A

Emotiv Inc. é uma empresa de bioinformática com sede em São Francisco. Ela desenvolveu fones de ouvido denominados "*Insight*", que monitoram as ondas cerebrais e captam as informações como dados sobre gestos, movimentos, preferências, tempos de reação e atividade cognitiva de quem os utiliza.

O autor alegou ter comprado um produto da empresa e ter autorizado o armazenamento de seus dados neurais que deveria ser feito de forma anônima apenas para finalidades científicas. Contudo, o autor afirmou que não houve a proteção adequada da privacidade das informações cerebrais, o que violaria garantias constitucionais previstas no artigo 19 da Constituição chilena, pois a empresa utilizou os dados para outras finalidades sem o seu consentimento, o que o expunha a riscos de reidentificação, hackeamento de seus dados, utilização e comercialização, entre outros.

A Emotiv Inc. sustentou que o autor manifestou seu consentimento de maneira livre e esclarecida, não havendo, em seu entendimento, violação de garantias constitucionais, já que o autor teria apenas indicado riscos hipotéticos e que a empresa disponibiliza canais para o cancelamento dos dados coletados. A Corte Chilena entendeu, por unanimidade, que as condutas realizadas violaram as garantias constitucionais contidas nos números 1 e 4 do artigo 19 da Constituição chilena, que se referem à integridade física e psíquica e ao direito à privacidade.

3.2.4 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.2.4.1 Rio Grande do Sul: Emenda Constitucional nº 85/2023

A Assembleia Legislativa do Estado do Rio Grande do Sul promulgou a Emenda Constitucional nº 85/2023, inserindo o parágrafo único do art. 235 da Constituição do Estado do Rio Grande do Sul, que passa a ter a seguinte redação:

> Art. 235. [...]
>
> Parágrafo único. A política e a pesquisa científica e tecnológica basear-se-ão no respeito à vida, à saúde, à dignidade humana, à integridade mental do ser humano e aos valores culturais do povo, na proteção, controle e recuperação do meio ambiente, e no aproveitamento dos recursos naturais.

3.2.4.2 Proposta de Emenda à Constituição Federal nº 29/2023

A Proposta de Emenda à Constituição nº 29/2023 visa incluir, entre os direitos e as garantias fundamentais, a proteção à integridade mental e à transparência algorítmica como requisitos para o desenvolvimento científico e tecnológico, com a seguinte redação: "Art. 5o. [...] LXXX – o desenvolvimento científico e tecnológico assegurará a integridade mental e a transparência algorítmica, nos termos da lei." (Senado Federal, 2023)

3.2.4.3 Projeto de Lei nº 1.229/2021

O Projeto de Lei nº 1.229/2021, apresentado na Câmara dos Deputados pelo deputado Carlos Henrique Gaguim, propõe alterações na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), com o objetivo de regulamentar os chamados neurodireitos e estabelecer diretrizes éticas para o uso de neurotecnologias.

O texto visa incluir, no art. 5º da LGPD, novas definições:

> Art. 5° [...]
> XX – dado neural: qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador invasivas ou não-invasivas;
> [...]
> XXI – interface cérebro-computador: qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo;
> XXII – neurotecnologia: conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso.

Além disso, o projeto propõe a criação de uma nova seção na LGPD, denominada Seção II-A – Do Tratamento de Dados Neurais e da Proteção dos Neurodireitos, contendo os seguintes dispositivos:

> Art. 13-A. O tratamento de dados neurais somente ocorrerá quando o titular ou o responsável legal consentir, de forma específica e destacada, para finalidades específicas, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente.
>
> Art. 13-B. É vedado o uso de qualquer interface cérebro-computador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua continuidade psicológica.
>
> Art. 13-C. É vedada a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica.
>
> Art. 13-D. O pedido de consentimento para o tratamento de dados neurais deve indicar, de forma clara e destacada, os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, os direitos do titular e os deveres do controlador e operador, as contraindicações bem como as normas sobre privacidade e as medidas de segurança da informação adotadas.
>
> Art. 13-E. Os dados neurais constituem uma categoria especial de dados sensíveis relacionados à saúde, os quais demandam maior proteção.
>
> Art. 13-F. Não se aplicam aos dados neurais as exceções previstas no art. 4º.

Art. 13-G. O Estado tomará medidas para assegurar o acesso equitativo aos avanços da neurotecnologia.

3.2.4.4 Projeto de Lei nº 522/2022

Com o objetivo de conceituar dado neural e regulamentar sua proteção, o Projeto de Lei nº 522/2022, também de autoria do deputado Carlos Henrique Gaguim, apresenta redação semelhante ao Projeto de Lei nº 1.229/2021 e propõe a modificação da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), que passaria a ter a seguinte redação:

> Art. 2o O caput do art. 5° da Lei n° 13.709, de 14 de agosto de 2018, passa a vigorar acrescido com as seguintes alterações:
>
> Art. 5° [...]
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, dado neural, quando vinculado a uma pessoa natural;
>
> [...]
>
> XX – dado neural: qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador, ou qualquer outra tecnologia, invasivas ou não-invasivas;
>
> XXI – interface cérebro-computador: qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo;
>
> XXII – neurotecnologia: conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso."
>
> Art. 3° O Capítulo II da Lei n° 13.709, de 14 de agosto de 2018, passa a vigorar acrescido da seguinte Seção II-A:
>
> "Seção II-A Do Tratamento de Dados Neurais
>
> Art. 13-A O tratamento de dados neurais somente ocorrerá quando:
>
> I - o titular ou o responsável legal consentir, de forma específica e destacada, para finalidades específicas, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais sensíveis;

b) proteção da vida ou da incolumidade física do titular ou de terceiro;

c) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Parágrafo único. O pedido de consentimento para o tratamento de dados neurais deve indicar, de forma clara e destacada, os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, as contraindicações bem como as normas sobre privacidade e as medidas de segurança da informação adotadas.

Art. 13-B É vedado o uso de qualquer interface cérebrocomputador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica.

Art. 13-C É vedada a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica.

Art. 13-D Não se aplicam aos dados neurais as exceções previstas no inciso I e inciso II, alínea 'a', do art. 4o.

Art. 13-E O Estado tomará medidas para assegurar o acesso equitativo aos avanços da neurotecnologia.

3.2.4.5 Projeto de Lei n.º 2.174/2023

O Projeto de Lei n.º 2.174/2023, de autoria do deputado Rubens Pereira Júnior, objetiva estabelecer normas e princípios para proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, a fim de garantir a proteção e promoção dos neurodireitos dos indivíduos, nos seguintes termos:

Art. 1o – Esta Lei estabelece as normas e princípios para proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, objetivando garantir a proteção e promoção dos neurodireitos dos indivíduos.

Art. 2o – Os Neurodireitos são os direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, incluindo, mas não se limitando a:

I – Direito à integridade cerebral e neurológica;

II – Direito à privacidade cerebral e neurológica;

III – Direito à liberdade cognitiva;

IV – Direito à igualdade cognitiva;

V – Direito à educação e à informação neurocientífica;

VI – Direito à autonomia pessoal e ao livre arbítrio;

VII – Direito à não discriminação baseada em características neurológicas.

Art. 3o – É dever do Estado garantir a proteção dos Neurodireitos, bem como promover medidas de prevenção e combate a violações desses direitos.

Art. 4o – Os Neurodireitos aplicam-se a todas as pessoas, independentemente de idade, gênero, orientação sexual, raça, religião, condição social ou quaisquer outras características pessoais.

Art. 5o – O direito à integridade cerebral e neurológica abrange o direito à proteção contra qualquer forma de intervenção ou modificação forçada do cérebro ou do sistema nervoso humano, bem como o direito à reparação em caso de dano neurológico.

Art. 6o – O direito à privacidade cerebral e neurológica abrange o direito à proteção contra a coleta, armazenamento, processamento, compartilhamento ou uso não autorizado de informações cerebrais ou neurológicas.

Art. 7o – O direito à liberdade cognitiva abrange o direito de pensar, imaginar, criar e expressar livremente ideias, conceitos, emoções e sentimentos, sem censura ou coerção.

Art. 8o – O direito à igualdade cognitiva abrange o direito de todas as pessoas terem as mesmas oportunidades de desenvolvimento cerebral e neurológico, sem discriminação de qualquer natureza.

Art. 9o – O direito à educação e à informação neurocientífica abrange o direito de todas as pessoas terem acesso a informações sobre o cérebro e o sistema nervoso humano, bem como o direito de receber educação em neurociência.

Art. 10o – O direito à autonomia pessoal e ao livre arbítrio abrange o direito de todas as pessoas de tomar suas próprias decisões e de controlar suas próprias experiências mentais, sem interferência externa.

Art. 11 – O direito à não discriminação baseada em características neurológicas abrange o direito de todas as pessoas de serem tratadas com igualdade e dignidade, independentemente de suas características neurológicas.

Art. 12 – É vedada a utilização de informações cerebrais ou neurológicas para fins discriminatórios ou ilegais.

Art. 13 – Fica estabelecido que todo indivíduo tem o direito de autonomia sobre seu próprio cérebro e sistema nervoso, bem como a integridade física e mental.

Art. 14 – É vedada a utilização de técnicas de modificação cerebral sem o consentimento livre, informado e esclarecido do indivíduo, exceto em casos de tratamentos médicos indispensáveis para preservação da vida ou saúde, desde que cumpridos os requisitos éticos e legais.

Art. 15 – É proibido o uso de técnicas de leitura de mente sem o consentimento do indivíduo.

Art. 16 – Fica estabelecido que todo indivíduo tem o direito à privacidade de suas atividades cerebrais, sendo proibido o monitoramento sem autorização ou ordem judicial.

Art. 17 – É vedada a utilização de técnicas de persuasão ou manipulação cerebral sem o consentimento livre, informado e esclarecido do indivíduo.

Art. 18 – Fica estabelecido que toda pesquisa envolvendo técnicas de modulação cerebral deve ser realizada de acordo com os princípios éticos e legais,

incluindo a obtenção de consentimento livre, informado e esclarecido do indivíduo de forma expressa e por escrito.

Art. 19 – É garantido o direito do indivíduo de acesso e controle sobre suas próprias informações cerebrais, sendo proibido o uso dessas informações sem autorização ou ordem judicial.

Art. 20 – Fica estabelecido que toda pessoa que violar os direitos estabelecidos nesta Lei estará sujeita às sanções penais e civis previstas na legislação brasileira.

3.2.5 Comentários sobre o texto do projeto da reforma do Código Civil

O Projeto de Lei nº 4, de 2025, ao incorporar os neurodireitos, objetiva assegurar a proteção dos direitos da personalidade no cenário das inovações tecnológicas, prevendo a possibilidade de regulamentação por leis específicas, bem como o uso e o acesso a dados cerebrais, desde que estejam mantidas as proteções e garantias relacionadas aos direitos de personalidade. Desta forma, visa trazer princípios gerais que irão balizar o processo de regulamentação, e, assim como ocorre com outros temas, não impede a criação de uma lei específica que irá detalhar a sua regulamentação[9].

O texto do PL 4/2025 estabelece que os neurodireitos constituem parte inalienável da personalidade humana, com a garantia de que são intransferíveis, irrenunciáveis e ilimitáveis. O legislador estabeleceu, portanto, que os neurodireitos integram a esfera dos direitos da personalidade, suprindo a necessidade de se realizar um esforço hermenêutico para aproximá-los de um dos outros direitos da personalidade, com um tratamento exclusivo para eles.

O parágrafo 1º do dispositivo conceitua os neurodireitos a partir de uma visão abrangente, que não se limita ao mero controle informacional, mas alcança dimensões estruturais da autonomia psíquica e da construção do self individual, tais como direitos destinados a proteger a privacidade mental, a identidade pessoal, o livre arbítrio, o acesso justo às tecnologias de aprimoramento cognitivo, a integridade mental e a proteção contra vieses derivados do uso de neurotecnologias.

O parágrafo 2º estabelece um rol exemplificativo de garantias específicas, que concretizam classificações praticadas internacionalmente, além de ampliar as classificações, dividindo os neurodireitos em:

a) direito à liberdade cognitiva;

b) direito à privacidade mental;

c) direito à integridade mental;

d) direito de continuidade da identidade pessoal e da vida mental, com a proteção contra alterações na identidade pessoal ou coerência de comportamento;

9 "§ 3º Os neurodireitos e o uso ou acesso a dados cerebrais poderão ser regulados por normas específicas, desde que preservadas as proteções e as garantias conferidas aos direitos de personalidade".

e) direito ao acesso equitativo a tecnologias de aprimoramento ou extensão das capacidades cognitivas;

f) direito à proteção contra práticas discriminatórias, enviesadas a partir de dados cerebrais.

A intervenção das tecnologias na tomada de decisão já está presente na sociedade, como os aplicativos dos aparelhos eletrônicos que armazenam as informações de navegação e as utilizam de maneira a influenciar a tomada de decisão dos indivíduos com os chamados "algoritmos". Com isso, é perceptível que se faz mister a proteção do livre-arbítrio como neurodireito autônomo, ao passo que as informações obtidas por meio das neurotecnologias podem ser utilizadas para influenciar as escolhas dos seres humanos.

Os dados neurais, derivados da análise da atividade mental, devem ser mantidos confidenciais, garantindo à pessoa de quem esses dados se originam o direito de apagá-los. Ademais, ao levar em consideração a privacidade mental, a atividade comercial, de qualquer natureza, deve ser minuciosamente regulamentada, de modo que as pessoas devem ter controle final em relação à sua própria tomada de decisão, livre de manipulação proveniente de tecnologias externas.

Já a proteção contra vieses é um neurodireito importante que tem, como base, o estabelecimento de normas para os algoritmos em neurotecnologia, sobretudo quando se utiliza a inteligência artificial. Tal problemática decorre do fato de que essas são abastecidas por uma base de dados provenientes da própria sociedade. A partir da perspectiva de que a inteligência artificial não detém o senso crítico para tratar das informações, gera-se a possibilidade de replicação dos preconceitos e vieses sociais quando as utilizam.

Assim, ao conceber os neurodireitos como direitos da personalidade no projeto de reforma do Código Civil, positivando-os em nosso ordenamento jurídico, estamos dando um passo fundamental para a proteção integral da pessoa humana, atualizando a sistemática legal defasada ante os constantes avanços tecnológicos e dirimindo os pontos de inseguranças jurídicas, que podem ser intensamente explorados pelas grandes empresas, o que reafirma os princípios preconizados na Carta Magna, como o da dignidade da pessoa humana.

3.3 Do direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo

O texto abaixo está contido no Capítulo IV do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Do direito ao ambiente digital transparente e seguro".

CAPÍTULO IV

DO DIREITO AO AMBIENTE DIGITAL TRANSPARENTE E SEGURO

Art. 2.027-U. É assegurado a todos o direito a um ambiente digital seguro e confiável, baseado nos princípios gerais de transparência, de boa-fé, da função social e da prevenção de danos.

Parágrafo único. As plataformas digitais devem demonstrar a adoção de medidas de diligência para garantir a conformidade dos seus sistemas e processos com os direitos de personalidade e os direitos à liberdade de expressão e de informação, incluindo a realização de avaliações de riscos sistêmicos para a mitigação e prevenção de danos.

Art. 2.027-V. As práticas de moderação de conteúdo devem respeitar a não discriminação e a igualdade de tratamento, a garantia da liberdade de expressão e a pluralidade de ideias, facilitando a prevenção e a mitigação de danos.

§ 1º As plataformas digitais devem demonstrar a adoção de medidas de diligência para mitigar e prevenir a circulação de conteúdo ilícito, nos termos do regulamento.

§ 2º Devem ser assegurados mecanismos eficazes de reclamação e de reparação integral de danos para permitir que as pessoas afetadas por conteúdo ilícito notifiquem a plataforma digital, por meio de acesso a canal de denúncias, em seu idioma local, devendo ser notificadas sobre o resultado de sua reclamação.

§ 3º Demonstrado o conhecimento pela plataforma sobre a potencial ilicitude do conteúdo, mediante notificação eletrônica do interessado, deverá ser adotadas as providências necessárias para a indisponibilização do conteúdo ilícito.

Art. 2.027-W. Os termos de uso das plataformas digitais devem ser elaborados de forma acessível, transparente e de fácil compreensão para todos, incluindo informações sobre as ferramentas, os sistemas e os processos usados para moderação e curadoria de conteúdo, incluindo informações sobre:

I – processos automatizados, realizados sem a intervenção humana;

II – formação de perfis pelo provedor por meio de técnicas de criação de perfis ou métodos similares;

III – existência de contrapartidas pecuniárias, como monetização ou patrocínio do conteúdo.

Parágrafo único. Os termos de uso das plataformas digitais e suas previsões que contrariarem normas cogentes ou de ordem pública serão nulos de pleno direito, nos termos do art. 166 deste Código.

Art. 2.027-X. As plataformas digitais de grande alcance devem identificar, analisar e avaliar, ao menos uma vez por ano, os seguintes riscos sistêmicos decorrentes da concepção ou do funcionamento de seu serviço:

I – a difusão de conteúdos ilícitos por meio de seus serviços;

II – os efeitos reais ou previsíveis em direitos de personalidade dos usuários, como consagrados pela Constituição da República Federativa do Brasil, por este Código Civil e por tratados internacionais de que o Brasil seja signatário;

III – os efeitos reais ou previsíveis que possam acarretar nos processos eleitorais e no discurso cívico;

IV – os efeitos reais ou previsíveis em relação à proteção da saúde e da segurança pública.

§ 1º O dever de realizar a avaliação periódica de riscos sistêmicos não se aplica aos provedores cuja atividade primordial seja:

I – o comércio eletrônico;

II – a realização de reuniões fechadas por vídeo ou voz;

III – o provimento de enciclopédias online, sem fins lucrativos;

IV – o provimento de repositórios científicos e educativos;

V – o desenvolvimento e compartilhamento de software de código aberto;

VI – prover serviços de busca e acesso a dados obtidos do Poder Público, em especial dos seus integrantes, conforme previsto em lei especial.

§ 2º Nas avaliações de risco, as plataformas digitais de grande alcance devem considerar a concepção de seus sistemas algorítmicos, os sistemas de moderação de conteúdo, os termos e políticas de uso, bem como os sistemas de seleção e de exibição de anúncios publicitários.

§ 3º As plataformas digitais de grande alcance devem, também, adotar as medidas necessárias para atenuar os riscos sistêmicos, considerando, especialmente, o impacto de tais medidas em direitos da pessoa.

§ 4º As medidas referidas no § 4º podem incluir a adaptação do funcionamento de seus termos e políticas de uso, a adaptação dos processos de moderação de conteúdo e dos sistemas de publicidade.

Art. 2.027-Y. As plataformas digitais de grande alcance estão sujeitas a auditorias anuais e independentes, por elas custeadas, para avaliar o cumprimento das obrigações deste Capítulo.

§ 1º As plataformas digitais de grande alcance devem cooperar com as organizações responsáveis pela auditoria independente, fornecendo a assistência necessária para que as auditorias sejam realizadas de maneira efetiva e eficiente, incluindo o acesso a dados relevantes e respostas a questionamentos.

§ 2º As auditorias independentes previstas neste artigo devem ser realizadas por entidades comprovadamente independentes, que não possuam conflitos de interesse com aquele que será auditado e que comprovem experiência, competência e capacidade técnica para gerenciamento de risco nas áreas auditadas.

§ 3º Cada auditoria deve produzir relatório fundamentado e por escrito, que inclua, pelo menos, as seguintes informações:

I – o nome, o endereço e o ponto de contato do fornecedor da plataforma sujeita à auditoria, bem como o período por ela abrangido;

II – o nome e o endereço das organizações que realizem a auditoria;

III – declaração de ausência de conflito de interesses;

IV – descrição dos elementos específicos auditados e da metodologia aplicada;

V – descrição e resumo das principais conclusões obtidas na auditoria;

VI – lista dos terceiros eventualmente consultados no processo de realização da auditoria;

VII – parecer que analise se o fornecedor da plataforma sujeita à auditoria cumpriu com as obrigações e compromissos referidos no caput deste artigo.

VIII – quando o resultado da auditoria não for positivo, recomendações operacionais sobre medidas específicas para que se alcance a conformidade exigida, no prazo recomendado.

§ 4° As plataformas digitais de grande alcance devem adotar as medidas necessárias para garantir o cumprimento das recomendações previstas no inciso VIII do § 3º deste artigo.

§ 5° As plataformas digitais de grande alcance devem, em até um mês do recebimento das recomendações previstas no inciso VIII do § 3º deste artigo, publicar relatório de implementação de auditoria, indicando quais medidas foram adotadas para solucionar os problemas indicados ou, na impossibilidade de implementá-las, a sua justificativa.

§ 6° As entidades responsáveis pela auditoria independente devem assegurar níveis adequados de confidencialidade e respeitar o sigilo dos atos e negócios das plataformas e dos terceiros quanto às informações obtidas na auditoria, inclusive após o seu término.

§ 7º Para fins de elaboração dos relatórios de transparência, o relatório da auditoria e o relatório da implementação de auditoria referidos nos §§ 4º e 6º deste artigo devem ser acompanhados de versões que não contenham qualquer informação que possa ser considerada como confidencial.

Art. 2.027-Z. As plataformas digitais podem ser responsabilizadas administrativa e civilmente:

I – pela reparação dos danos causados por conteúdos gerados por terceiros cuja distribuição tenha sido realizada por meio de publicidade da plataforma;

II – por danos decorrentes de conteúdos gerados por terceiros, quando houver descumprimento sistemático dos deveres e das

> obrigações previstas neste Código, aplicando-se o sistema de responsabilidade civil nele previsto.

3.3.1 Abordagem teórica da temática

Por meio da estrutura da tecnologia em rede, característica da internet, e considerando a estrutura social inerente à sociedade capitalista, as plataformas digitais emergiram como o principal espaço para a realização de atividades econômicas, sociais, culturais e políticas no século XXI. Elas fornecem uma infraestrutura digital que facilita a interação entre diversos atores, como usuários, clientes, consumidores, eleitores, anunciantes, vendedores, prestadores de serviços, produtores e fornecedores, o que permite o registro de dados e metadados relacionados a essas interações.

Para uma análise sólida desse novo marco normativo, é imperativo delimitar os desafios impostos pela ambiência digital. A inserção de um novo meio – tecnodigital – no estabelecimento de relações jurídicas altera, por si só, as dinâmicas entre os sujeitos, aspecto denominado pelo legislador reformador de "situações jurídicas no ambiente digital". Além disso, o novo meio digital potencializa o surgimento de novos tipos de conflitos sociais, que derivam do ambiente tecnológico, e não propriamente da relação jurídica.

As plataformas digitais podem ser categorizadas a depender da atividade a que se destinam e, de forma exemplificativa, podem atender a diferentes utilidades, tais como mídia social, de conteúdo, comércio eletrônico, serviços, finanças e pagamentos, saúde digital, educação on-line, entre outras.

Especial atenção deve ser dada às plataformas digitais de conteúdo, pois deixaram de ser meros repositórios de informações para atuar como "editoras" de conteúdo, com um papel mais ativo no gerenciamento e curadoria do que é apresentado aos usuários, o que impacta em suas responsabilidades e exige uma reflexão aprofundada sobre a sua influência na sociedade.

Como "editoras", essas plataformas não apenas armazenam e distribuem informações, mas também influenciam o tipo de conteúdo que ganha relevância e visibilidade. Nesse sentido, Luís Roberto Barroso e Luna Van Brussel Barroso (2023) afirmam que:

> A internet, com o surgimento de sites, blogs pessoais e redes sociais, revolucionou esse universo. Criou comunidades on-line para disseminação de textos, imagens, vídeos e links gerados pelo usuário, publicados sem controle editorial e sem custo. Tais inovações amplificaram o número de pessoas que participam do debate público, diversificaram as fontes de informação e aumentaram exponencial- mente o acesso a elas. Essa nova realidade deu voz às minorias, à sociedade civil, aos políticos, aos agentes públicos, aos influenciadores digitais e permitiu que as demandas por igualdade e democracia adquirissem dimensões globais. Tudo isso representou uma poderosa contribuição para o

dinamismo político e a resistência ao autoritarismo, e estimulou a criatividade, o conhecimento científico e as trocas comerciais. Cada vez mais, as comunicações políticas, sociais e culturais relevantes ocorrem através desse meio.

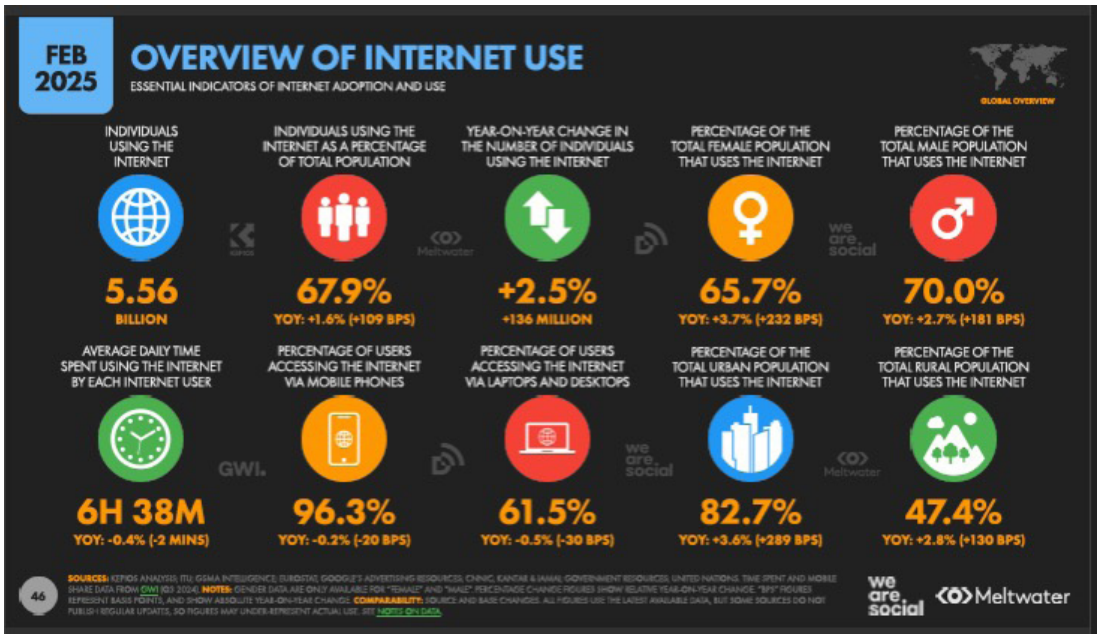
No entanto, o surgimento das redes sociais também levou a um aumento exponencial na disseminação de discurso abusivo e criminoso. Embora essas plataformas não tenham criado desinformação, discursos de ódio ou discursos que atacam a democracia, a capacidade de publicar livremente, sem controle editorial e com pouca ou nenhuma responsabilidade, aumentou o uso dessas táticas. Além disso, e mais fundamentalmente, os modelos de negócio das plataformas agravaram o problema pela utilização de algoritmos que controlam e distribuem conteúdo on-line.

Atualmente, a ampliação do engajamento on-line é determinada pelos algoritmos das grandes empresas de tecnologia. Embora inicialmente essas plataformas digitais tenham se apresentado como espaços neutros, onde os usuários poderiam publicar livremente, elas assumem papéis legislativos, executivos e judiciais. Isso ocorre porque (i) estabelecem de forma unilateral as regras de discurso em seus termos de uso, (ii) através de algoritmos controlam a distribuição e moderação do conteúdo, e (iii) determinam como essas regras serão implementadas[10].

10 "Especificamente, as plataformas digitais dependem de algoritmos para duas funções diferentes: recomendar e moderar conteúdo. Primeiramente, um aspecto fundamental do serviço que oferecem envolve a curadoria do conteúdo disponível, de modo a proporcionar a cada usuário uma experiência personalizada e aumentar o tempo gasto on-line. Elas recorrem a algoritmos de deep learning que monitoram cada ação na plataforma, extraem dados e preveem qual conteúdo manterá um usuário específico engajado e ativo, com base em sua atividade anterior ou de usuários semelhantes. A transição de um mundo de escassez de informação para um mundo de abundância de informação gerou uma concorrência acirrada pela atenção do usuário – esse, sim, o recurso escasso na era digital. Portanto, o poder de modificar o ambiente informacional de uma pessoa tem um impacto direto no seu comportamento e nas suas crenças. E como os sistemas de IA podem rastrear o histórico on-line de um indivíduo, eles podem adaptar mensagens específicas para maximizar o impacto. Mais importante ainda, eles monitoram como o usuário interage com a mensagem personalizada, utilizando esse feedback para influenciar a segmentação de conteúdo futuro, tornando-se cada vez mais eficazes na moldagem de comportamentos. Dado que os seres humanos se envolvem mais com conteúdo polarizador e provocativo, esses algoritmos acabam por provocar emoções fortes, incluindo raiva. O poder de organizar o conteúdo on-line, portanto, tem impactos diretos sobre a liberdade de expressão, o pluralismo e a democracia. Além dos sistemas de recomendação, as plataformas também dependem de algoritmos para a moderação de conteúdo, que consiste na prática de classificar o conteúdo para verificar se viola os padrões da comunidade. Como mencionado, o crescimento das redes sociais e seu uso por pessoas ao redor do mundo permitiram a propagação da ignorância, mentiras e a prática de crimes de diferentes naturezas com pouco custo e quase nenhuma responsabilização, ameaçando a estabilidade até mesmo de democracias duradouras. Nesse cenário, tornou-se inevitável a criação e imposição de termos e condições que definem os valores e normas que cada plataforma deseja para sua comunidade digital e que pautarão a moderação do discurso. Mas a quantidade potencialmente infinita de conteúdo publicado on-line significa que esse controle não pode ser exercido exclusivamente por seres humanos. Algoritmos de moderação de conteúdo otimizam a varredura do material publicado on-line para identificar violações dos padrões da comunidade ou termos de serviço em escala e aplicar medidas que variam desde remoção até redução/ amplificação do alcance ou inclusão de esclarecimentos ou referências a infor- mações alternativas. As plataformas frequentemente dependem de dois modelos algorítmicos para moderação de conteúdo. O primeiro é o modelo de detecção de reprodução, que usa o hashing, uma tecnologia que atribui um ID único a textos, imagens e vídeos, para identificar reproduções idênticas de conteúdo previamente rotulado como indesejado. O segundo sistema, o modelo preditivo, usa técnicas de machine learning para identificar potenciais ilegalidades em conteúdo novo e não classificado. O machine learning é um subtipo de inteligência artificial que depende de algoritmos treinados em vez de programados, capazes de aprender a partir de dados sem codificação explícita. Embora úteis, ambos os modelos

O relatório "Digital 2025: Global Overview Report", elaborado pela We Are Social e Hootsuite, fornece dados sobre o uso da internet no mundo, como se verifica abaixo.

Figura 4 – Dados gerais sobre o uso da internet

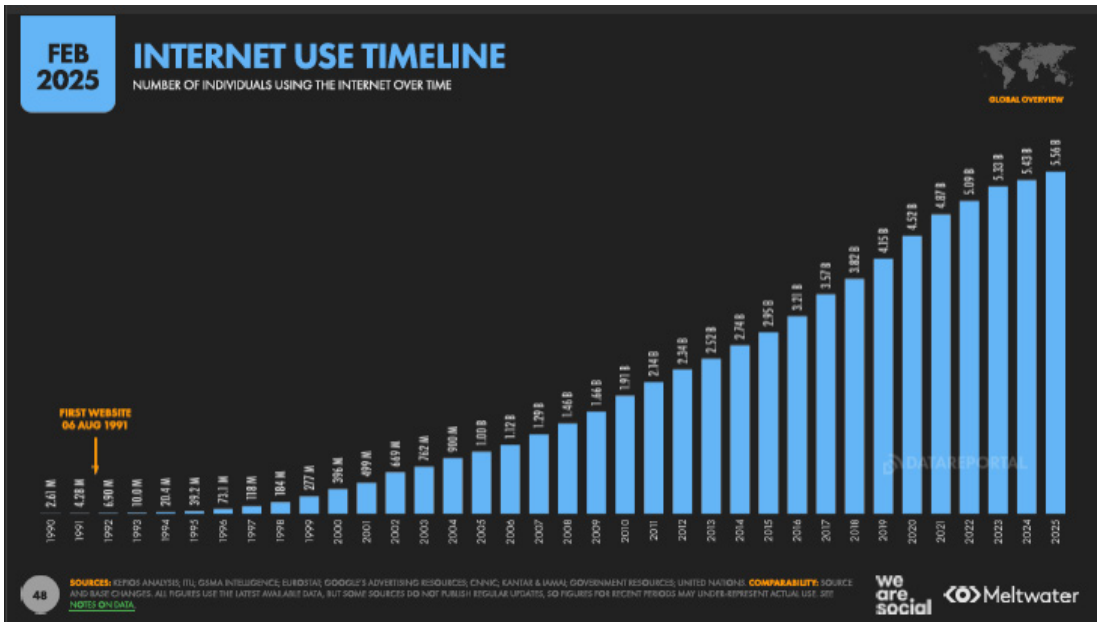


Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

Segundo o referido relatório, mais de 5 bilhões de pessoas usam a internet, o que corresponde a 67% da população mundial. No gráfico abaixo, verificamos a curva ascendente na série evolutiva do tempo dispendido na internet:

têm limitações. O modelo de detecção de reprodução é ineficiente para conteúdo como discurso de ódio e desinformação, em que o potencial de novas e diferentes publicações é praticamente ilimitado e os usuários podem fazer alterações deliberadas para evitar a detecção. O modelo preditivo, por sua vez, ainda é limitado em sua ca- pacidade de lidar com situações às quais não foi exposto durante o treinamento, principalmente por uma incapacidade de entender significados e levar em conta considerações contextuais que influenciam a legitimidade do discurso. Além disso, os algoritmos de machine learning também dependem de dados coletados do mundo real e podem incorporar preconceitos ou vieses, levando a aplicações assimétricas do filtro. E como os conjuntos de dados de treinamento são muito grandes, é difícil auditá-los para detectar essas falhas. Apesar dessas limitações, os algoritmos continuarão a ser um recurso crucial no monitoramento de conteúdo, dada a escala das atividades on-line". (Barroso; Barroso, 2023, p. 291-293).

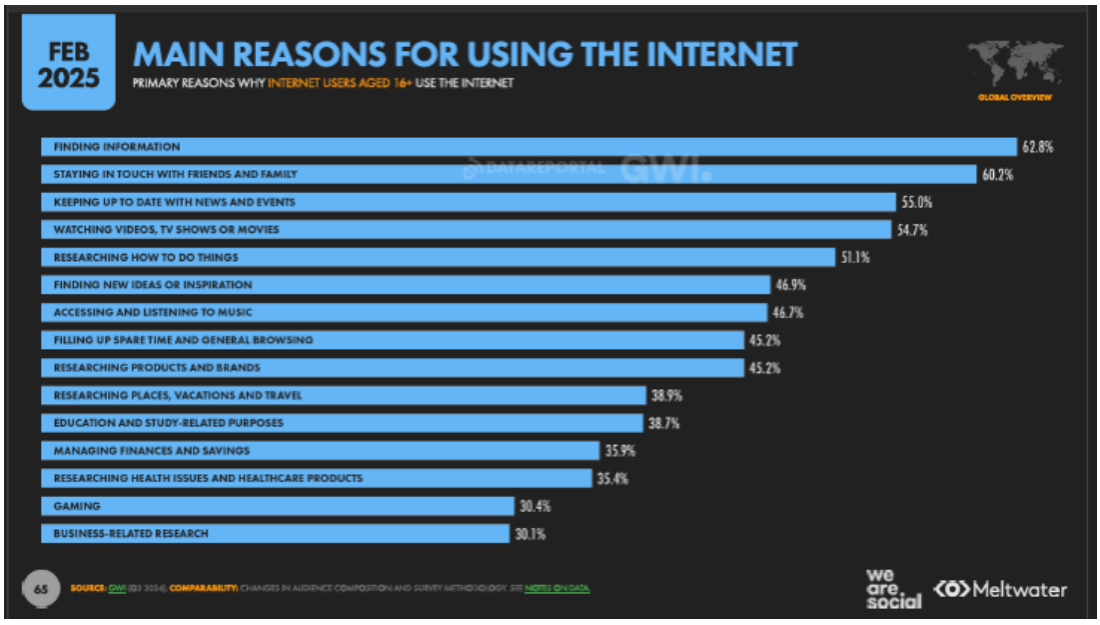
Figura 5 – Dados sobre o tempo de uso da internet



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025..

Entre as razões para o uso da internet, a maior motivação é "buscar informações", com 62,8% dos usuários adultos afirmando que essa é uma das principais razões para usar a internet hoje, seguida por "manter contato com amigos e familiares", como se verifica abaixo.

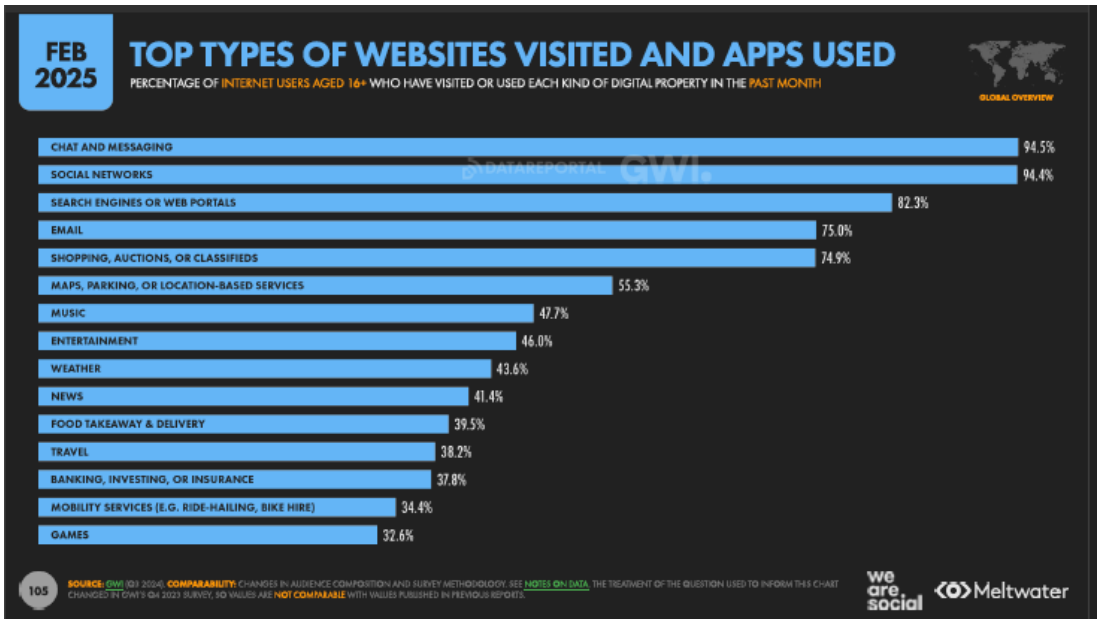
Figura 6 – Dados sobre os motivos para usar a internet



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

Os chats e aplicativos de mensagens (94,5%), bem como as redes sociais (94,4%) ficam no topo dos websites e aplicativos utilizados, como se verifica abaixo.

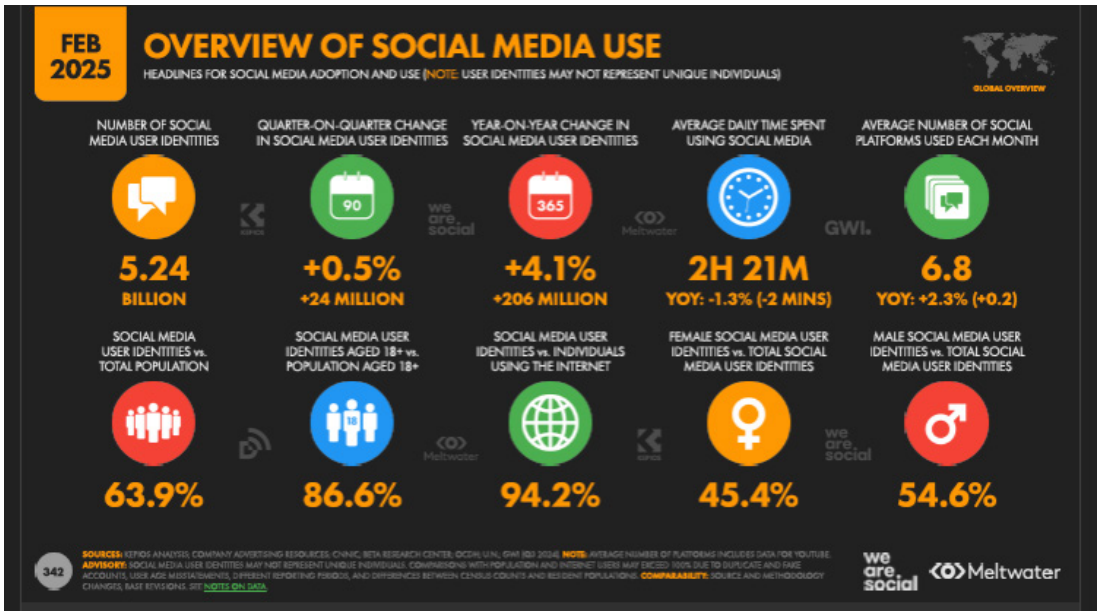
Figura 7 – Ranking dos websites e aplicativos mais acessados



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

No âmbito das redes sociais, o relatório identifica a existência de mais de 5 bilhões de perfis, com um tempo médio diário de acesso de mais de duas horas, como se verifica abaixo.

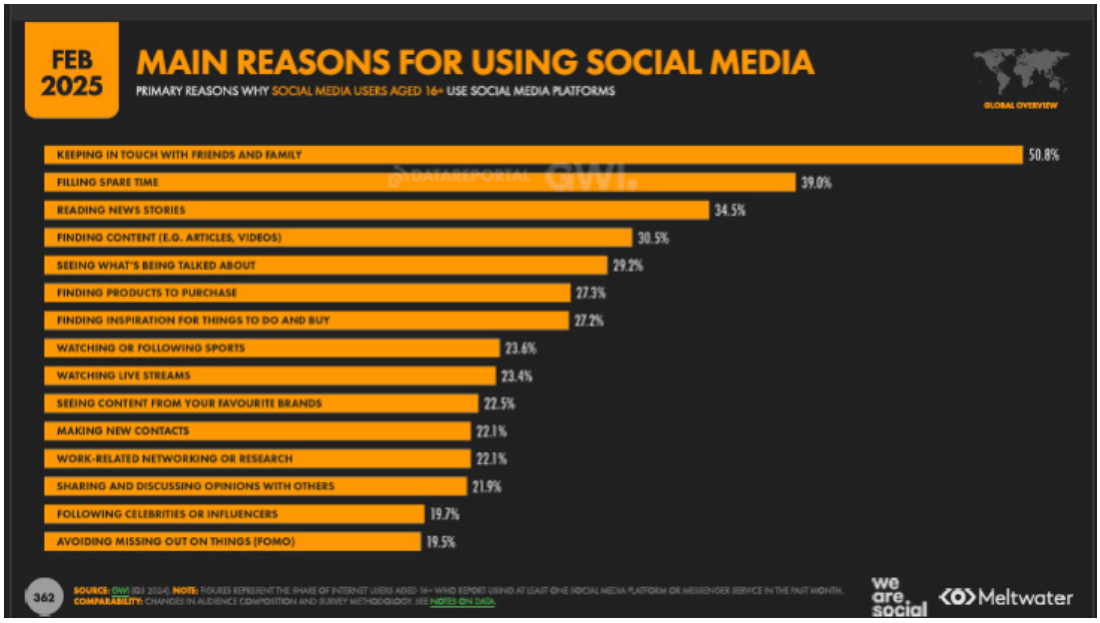
Figura 8 – Dados gerais sobre o uso das redes sociais



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

Entre as razões para o acesso às redes sociais, a maior motivação é "manter contato com amigos e familiares", com 50,8% dos usuários afirmando que essa é uma das principais razões para usá-las, como se verifica abaixo.

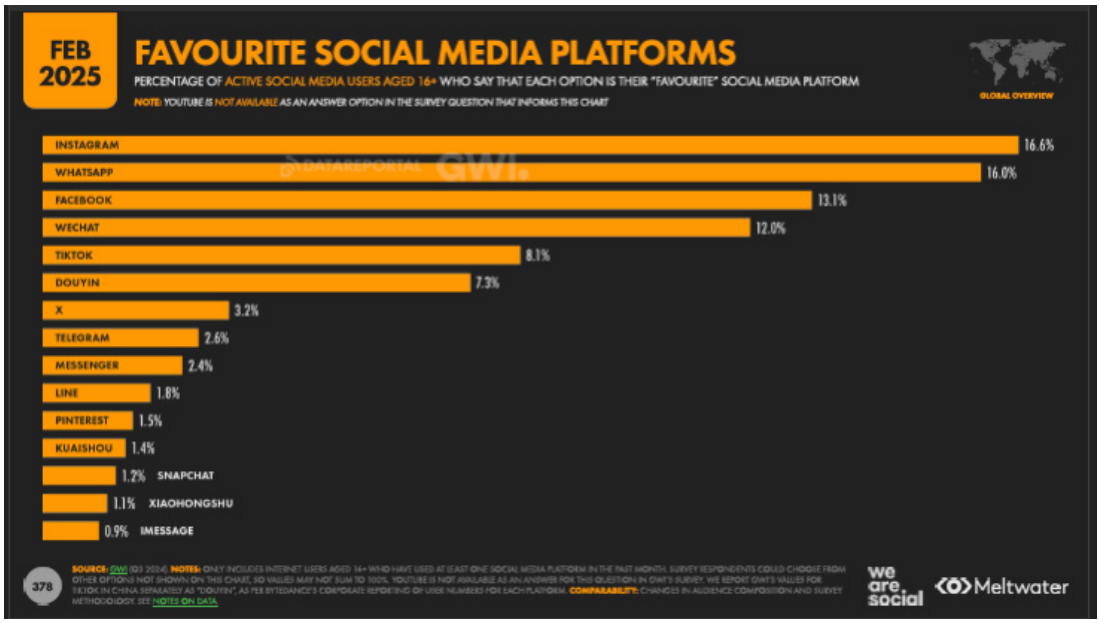
Figura 9 – Dados sobre os motivos para usar as redes sociais



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

Entre as plataformas de mídia social, as três mais utilizadas são Instagram, WhatsApp e Facebook, como se verifica abaixo.

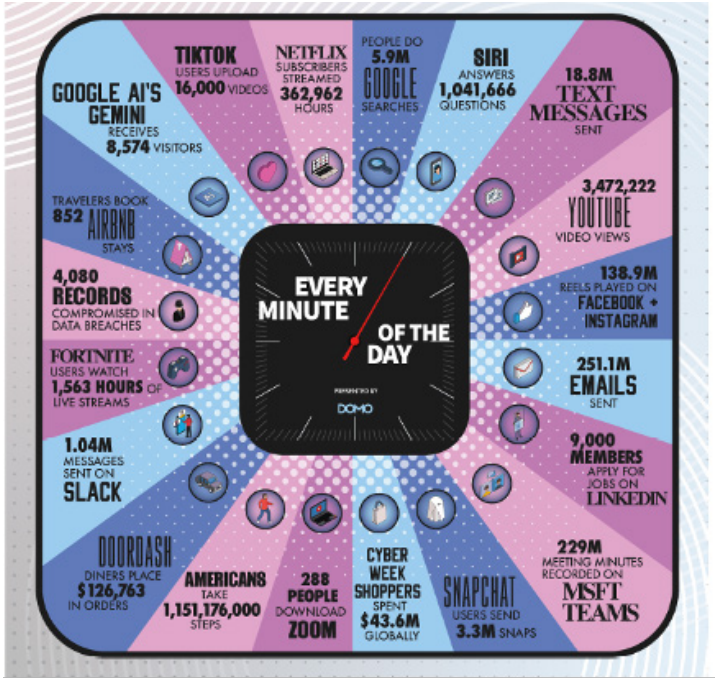
Figura 10 – Ranking das plataformas de redes sociais mais acessadas



Fonte: WE ARE SOCIAL; MELTWATER. Digital 2025: Global Overview Report. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

No 12º Relatório "Data Never Sleeps" publicado pela Domo, é possível verificar a quantidade de dados gerada a cada minuto:

Figura 11 – Infográfico do 12º Relatório "Data Never Sleeps"



Fonte: Domo – infographic Data Never Sleeps 12.0. Disponível em: https://www.domo.com/learn/infographic/data-never-sleeps-12?utm_source=wire&utm_medium=pr&utm_campaign=PR_Domo_Data_Never_Sleeps_12&campid=701Vq000001ztWzIAI

Os dados acima ilustram o fenômeno denominado "plataformização da vida" (Van Dijck; Poell; de Wall, 2018), no qual as plataformas digitais se tornam essenciais para a organização e mediação de várias esferas da vida cotidiana, o que revela a centralidade e relevância da normatização com importantes impactos sociais, econômicos e políticos. Esse fenômeno tem levado diversos ordenamentos jurídicos a editar diferentes normas para regulação das plataformas digitais, algumas das quais serão brevemente analisadas a seguir.

3.3.2 Experiências normativas do direito estrangeiro e transnacional

3.3.2.1 União Europeia

Na União Europeia, a legislação é mais uniforme e sofisticada, considerando a convencionalidade de natureza transnacional. Nesse sentido, no tocante à regulamentação das plataformas digitais, destacam-se:

a) Regulamentação para a proteção da privacidade e dos dados, pelo Regulamento Geral de Proteção de Dados (GDPR):

O Regulamento Geral de Proteção de Dados (GDPR, da sigla em inglês), em vigor desde 2018, estabeleceu um marco regulatório inovador para a proteção de dados pessoais. Entre os principais pilares da norma – que inspirou amplamente a pela Lei Geral de

Proteção de Dados Pessoais brasileira, a LGPD – estão a responsabilização dos controladores de dados, a imposição de deveres de transparência, e o fortalecimento dos direitos dos titulares de dados. As plataformas passaram, dessa forma, a ter obrigações específicas relacionadas à coleta, armazenamento, tratamento e compartilhamento de informações pessoais de seus usuários.

Além disso, introduziu requisitos como o consentimento explícito para o tratamento de dados, o direito ao apagamento, a portabilidade dos dados e o dever de notificação em caso de violação de segurança dos dados. Também impôs a adoção de medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais. Especificamente, no caso das grandes plataformas digitais, essas obrigações ganharam proporções mais significativas, pois o volume de dados tratados e o potencial de risco à privacidade dos usuários são significativamente maiores. Outro aspecto central e merecedor de destaque do GDPR foi a criação de mecanismos para garantir a *accountability* das plataformas, incluindo a obrigatoriedade de realizar avaliações de impacto sobre a proteção de dados (*Data Protection Impact Assessment – DPIA*, da sigla em inglês) em casos de tratamentos de dados considerados de alto risco.

b) Regulamentação para a proteção do meio ambiente digital, pelo Digital Services Act (DSA), desde 2023, que estabelece obrigações para plataformas digitais, incluindo a remoção rápida de conteúdos ilegais e transparência em algoritmos:

O Digital Services Act (DSA), em vigor desde 2023, objetiva estabelecer um equilíbrio entre liberdade de expressão, segurança digital e proteção de direitos fundamentais na União Europeia. O DSA adota um regime de obrigações graduais, com deveres mais rigorosos para as chamadas Very Large Online Platforms (VLOPs), especialmente no que diz respeito à gestão de riscos sistêmicos. Um ponto relevante é que a introdução pelo DSA de um formato escalonado de estabelecimento de obrigações às plataformas digitais, que impõe diferentes deveres de diligência proporcionalmente ao tamanho e ao impacto da plataforma.

Podemos destacar a busca pelo equilíbrio entre liberdade de expressão, segurança digital e proteção de direitos fundamentais na União Europeia. O DSA adota um regime de obrigações graduais, com deveres mais rigorosos para as chamadas *Very Large Online Platforms* (VLOPs), especialmente no que diz respeito à gestão de riscos sistêmicos. Um ponto relevante é que a introdução pelo DSA de um formato escalonado de estabelecimento de obrigações às plataformas digitais, que impõe diferentes deveres de diligência proporcionalmente ao tamanho e ao impacto da plataforma.

Entre os pontos centrais do Regulamento, podemos destacar a obrigação de rápida remoção de conteúdos ilegais, bem como maior transparência na operação de algoritmos e a exigência de auditorias independentes sobre o cumprimento das obrigações.

c) Regulamentação contra a prática anticoncorrencial, pelo Digital Markets Act (DMA), que estabelece legislação antitruste para grandes plataformas, chamadas de *gatekeepers*:

O Digital Markets Act (DMA), em vigor desde 2024, objetiva reequilibrar o poder de mercado no ambiente digital, especialmente no que diz respeito às grandes plataformas. Entre as obrigações, podemos destacar, por exemplo, a proibição da autopreferência nos resultados de busca e a exigência de que gatekeepers permitam a interoperabilidade de seus serviços.

d) Regulamentação para a proteção de direitos autorais no mercado digital, que visa responsabilizar plataformas por violação de direitos autorais, introduzindo o conceito de *upload filters*, que bloqueia conteúdos que infrinjam direitos autorais:

A Diretiva de Direitos Autorais no Mercado Único Digital, de 2019, cujo objetivo é reequilibrar a relação entre titulares de direitos e plataformas digitais, trouxe a exigência de que plataformas de compartilhamento de conteúdo on-line implementem filtros prévios, os conhecidos *upload filters*, para impedir a publicação de material que infrinja direitos autorais. O novo regime supera a lógica anterior de mera isenção de responsabilidade passiva prevista na Diretiva de Comércio Eletrônico.

e) Regulamentação contra a malversação da inteligência artificial, pelo AI Act com base no risco associado à tecnologia, com o estabelecimento de obrigações e condutas concretas, em extensa legislação:

Aprovado em 2024 pela União Europeia, o AI Act estabelece um marco regulatório robusto para o uso da inteligência artificial, a partir do modelo de gerenciamento de riscos com uma abordagem regulatória ex ante, classificando os sistemas de IA em diferentes categorias de risco (baixo, limitado, alto e inaceitável).

O regulamento estabelece critérios objetivos para a identificação e classificação dos sistemas de IA "de alto risco", bem como prevê normas mais rígidas tais sistemas, inclusive com requisitos técnicos e organizacionais para seu desenvolvimento e uso. Ademais, o AI Act determina a criação do Comitê Europeu para Inteligência Artificial (*European Artificial Intelligence Board*), cujo propósito é harmonizar a implementação das disposições do regulamento em todos os Estados-membros da UE. Importa destacar ainda que o regulamento traz uma série de requisitos de transparência e *accountability* para sistemas de IA generativa, com o propósito de incrementar o controle público sobre a tecnologia.

3.3.2.2 Estados Unidos

Os marcos mais relevantes sobre a regulamentação jurídica das plataformas digitais nos Estados Unidos são fragmentados, em decorrências das peculiaridades federativas do país, sendo influenciada por leis federais e estaduais e divididas entre (i) normas regulamentadoras dos serviços de hospedagem virtual e responsabilidade civil no âmbito da tecnologia digital e das plataformas digitais, seja em decorrência do design das ferramentas digitais, seja em decorrência da difusão ou moderação de conteúdos digitais; (ii) normas sobre proteção de dados pessoais e privacidade; (iii) normas de proteção aos

direitos autorais; e (iv) normas da legislação antitruste, mormente pelas práticas anticoncorrenciais de grandes plataformas digitais.

No contexto federal, a Seção 230 do *Communications Decency Act (CDA)* (Estados Unidos da América, 1996) protege plataformas digitais de responsabilidade legal por conteúdos gerados por terceiros, excetuando conteúdos ilegais, como pornografia infantil, atos obscenos, excessivamente violentos, assediantes ou outra forma de licitude questionável. Há discussões em curso em projetos de lei nos Estados Unidos sobre a necessidade de aprofundar a moderação e responsabilidade das plataformas em caso de discursos de ódio ou conteúdos ilícitos, com a revisão da supracitada seção. A Seção 230 estabelece, atualmente, a isenção de responsabilidade dos provedores, que não devem ser equiparados a um editor ou orador que realizou o discurso eventualmente ilícito ou danoso via plataforma digital. Nesse sentido, é a letra da lei 47 U.S.C. § 230, (c)(1): "Nenhum provedor ou usuário de um serviço de computador interativo será tratado como editor ou orador de qualquer informação fornecida por outro provedor de conteúdo de informação".[11] (Tradução nossa)

Enquanto determinados segmentos sociais e políticos reclamam uma maior moderação de conteúdo com a expectativa de responsabilização das plataformas digitais, como nos casos dos precedentes supracitados, há leis estaduais e projetos de lei regulamentando a questão em sentido contrário: pela liberdade de expressão e com menores restrições na moderação de conteúdo.

A seguir, elencamos alguns projetos de lei em tramitação nos Estados Unidos:

(i) Regulamentação federal das plataformas para proteção da infância e adolescência (*Kids Online Safety Act HR7891; Children and Teens' Online Privacy Protection Act HR 7890; Kids Online Safety and Privacy Act KOSPA*, versão combinada pelo Senado americano dos dois projetos anteriores). Sobre o tema, há ainda a legislação estadual, como o Código de Design Adequado à Idade da Califórnia (CAADCA), que foi originalmente impugnado, sob o ponto de vista constitucional, por suposta violação à Primeira Emenda pela *NetChoice* no final de 2022 (*NetChoice v. Bonta*). Há, ainda, o Stop Addictive Feeds Exploitation (SAFE) for Kids Act (HB7694) de Nova York e o Protecting Our Kids from *Social Media Addiction Act* (SB 976) da Califórnia, que proíbem plataformas de fornecer plataformas digitais com design de "feed viciante" para menores de 18 anos. Mais um exemplo é o Minnesota *Age-Appropriate Design Code Act*. Um relatório de 2023 da Universidade da Carolina do Norte em *Chapel Hill* fez uma análise da regulamentação das plataformas digitais quanto à proteção da infância, à privacidade, à moderação de conteúdo, ao uso de inteligência artificial, às práticas anticoncorrenciais e à taxação tributária das plataformas digitais. Diagnosticou-se que 13 estados americanos aprovaram um total de 23 leis sobre o design e a segurança on-line de crianças. Ainda, Tim Bernard (2023) identificou 144 projetos de lei focados na segurança on-line de crianças, propostos em legislaturas estaduais, em procedimento bicameral.

11 No original: "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*".

(ii) O projeto exige um algoritmo transparente, mas omite-se quanto à exigência de explicabilidade do design ou à proibição de um feed algorítmico engajador, pois se restringe a exigir transparência e a oferecer alternativas ao usuário. Em outros termos, o algoritmo pode ser transparente, mas ainda assim prejudicial, não havendo no projeto de lei, um arsenal legislativo que permita ao usuário exigir que a plataforma forneça opções alternativas de organização de conteúdo no feed ou de design da plataforma – seja organizado segundo os critérios preferenciais do usuário, seja com base em uma ordenação meramente cronológica da rede. Dessa forma, organizado segundo os critérios preferenciais do usuário ou, ainda, um critério meramente cronológico de ordenação da rede. Sobre o tema, há uma demanda relevante e massiva, em litisconsórcio de 42 procuradores-gerais estaduais, que alegam um design prejudicial da tecnologia digital em desfavor dos mais jovens: 33 procuradores-gerais estaduais entraram com uma demanda multiestadual (*multidistrict litigation*) (Estados Unidos da América, 2023) e em litisconsórcio contra a empresa Meta, na Corte Distrital do Distrito Norte da Califórnia, enquanto o estado de Massachusetts e mais outros oito estados entraram com ações nos próprios tribunais estaduais, valendo-se das mesmas alegações.

(iii) Regulamentação federal para proteção da soberania digital, em face de empresas estrangeiras de plataformas digitais, com acesso a dados pessoais e comportamentais dos americanos: Lei de Proteção aos Americanos Contra Adversários Estrangeiros – HR 7521 (2024) que implicaria a alienação do *TikTok*, o aplicativo de mídia social de propriedade da empresa chinesa *Bytedance*. Na ausência de uma alienação, caberá o banimento das lojas de aplicativos dos EUA e a proibição de ser hospedado nas fronteiras dos EUA. Essa lei ensejou o movimento "*TikTok ban*" (Castello, 2023), nos Estados Unidos, o que implicaria o banimento dessa plataforma digital para download e uso pelos americanos.

(iv) Regulamentação federal para a proteção contra a malversação da inteligência artificial e o uso de *deepfakes* geradas por inteligência artificial em plataformas digitais: 21 estados americanos já promulgaram pelo menos uma lei que criminaliza ou estabelece a responsabilidade civil em razão da disseminação de *deepfakes* em plataformas digitais, havendo atualmente 50 leis já promulgadas (Public Citizen, 2024). Não há acordo semântico ou uniformidade sobre o tema entre as legislações estaduais, tampouco sobre os requisitos suficientes para a responsabilização das plataformas digitais.

(v) Regulamentação para a proteção contra o design perverso ou enganador aos usuários digitais: H.R.7766 – *Protecting Consumers from Deceptive AI Act*. Há ainda a legislação estadual como *Deceptive Consumer Sales Act*, de Indiana.

(vi) Regulamentação federal para a proteção de direitos autorais em plataformas digitais: o *Digital Millennium Copyright Act* (DMCA), ao tratar da responsabilidade de plataformas sobre a proteção de direitos autorais.

(vii) Regulamentação federal para a proteção contra práticas anticoncorrenciais na legislação antitruste, vigoram as normas dos diplomas *Sherman Act* (1890), *Clayton Act*

(1914) e *Federal Trade Commission Act* (1914) constituem a base para ações regulatórias contra práticas anticompetitivas de grandes plataformas digitais, como Google e Meta, como foram as ações do FTC – *Federal Trade Comission* contra a Meta (2023).

Nota-se, portanto, que, apesar de fragmentada e polarizada, a legislação estadunidense enfrenta, no tocante às plataformas digitais, questões como (i) a proteção contra a malversação da inteligência artificial nas plataformas; (ii) a proteção da infância e adolescência; (iii) a proteção contra o design enganador na arquitetura digital; (iv) a proteção contra as práticas anticoncorrenciais e (v) a proteção contra a violação de direitos autorais.

3.3.2.3 Reino Unido

No Reino Unido, mais especificamente, fora do bloco da União Europeia, há o *UK Online Safety Act* de 2023. Trata-se de uma legislação abrangente, visando à proteção do usuário, em especial das crianças e dos adolescentes, a reprimir "conteúdo terrorista", conteúdo ilegal ou conteúdo legal, mas "prejudicial", e publicidade com design tecnológico enganador. Há, ainda, o *Age Appropriate Design Code* (2020), que estabelece parâmetros seguros de algoritmos e design digital para a criação de artefatos digitais protetivos da infância e adolescência.

3.3.2.4 Síntese analítica das experiências normativas de direito estrangeiro e transnacional

O Projeto de Lei nº 4, de 2025, aproxima-se do modelo europeu e britânico, ao prever deveres de transparência algorítmica, avaliação de riscos, auditorias independentes e procedimentos claros de moderação. Já o modelo estadunidense traz uma regulamentação fragmentada e influenciada pela Primeira Emenda que protege a liberdade de expressão.

3.3.3 Estudos de caso

3.3.3.1 Brasil: teses vigentes no STJ sobre moderação de conteúdo

O estudo (Salomão; Leme, 2024) realizado pela FGV Justiça, em 2024, em parceria com a Associação de Magistrados Brasileiros (AMB), o Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), o Jusbrasil e a FGV Comunicação Rio, analisou as decisões do STJ sobre a moderação de conteúdo em plataformas digitais, focando os Recursos Especiais para desvendar as tendências e direções adotadas pela corte.

O processo de coleta de dados foi iniciado de agosto de 2023 até janeiro de 2024, com uma pesquisa abrangente no JusBrasil, com a utilização do seguinte termo de busca: "*Marco civil da internet*". Foram estabelecidos critérios claros de inclusão e exclusão, focando em decisões de maior impacto ou que estabeleceram precedentes significativos. O período de análise foi ampliado para captar as tendências emergentes ao longo do

tempo. Essa pesquisa preliminar encontrou um total de 191 decisões (incluindo acórdãos e decisões monocráticas), entre 2015 e 2023, que continham o termo de busca. Objetivou-se centrar as análises somente em Recursos Especiais já julgados. Portanto, das 191 decisões que versavam sobre o MCI, foram selecionados 37 Recursos Especiais já julgados que envolviam casos em que a moderação de conteúdo foi o tema central.

Aplicando o método quantitativo, cada uma dessas decisões foi examinada no seu inteiro teor, levando em consideração as informações: *Autor; Autor menor; Réu; Tipo de ação; Relator; Turma; Unidade da Federação de origem do processo; Ano do ajuizamento; Data da decisão; Pedido; Fundamento do pedido; Os dispositivos legais do Marco Civil da Internet citados na decisão; e a Temática central da decisão*.

O estudo qualitativo das decisões teve o objetivo de consolidar as seguintes informações: Autor; Autor menor; Réu; Tipo de ação; Relator; Turma; Unidade da Federação de origem do processo; Ano da propositura da ação; Ano do julgamento do recurso especial; Pedido; Fundamentação do pedido; Dispositivos legais do marco civil da internet citados na decisão; Temática central da decisão; Resumo do caso; Ementa; Resultado do julgamento; Trechos dos votos separados por áreas temáticas; Outros julgados referenciados na decisão; Referências bibliográficas citadas na decisão.

Esse estudo apresenta o panorama sobre o tratamento do tema no STJ no período entre 2015 e 2023. Os dados refletem um aumento progressivo na quantidade de casos ao longo dos anos, iniciando com apenas uma decisão em 2015 e crescendo para sete em 2017 e em 2021. Observa-se uma leve redução em 2018, 2019, 2020, 2022 e 2023, com até cinco casos.

Dos 37 Recursos Especiais analisados, observou-se uma diversidade de focos, porém os temas mais comuns foram: "Prestação de informações para identificação do autor do ato ilícito", "Individualização da URLS - Requisitos de validade da ordem judicial" e "Veiculação de fotografia de imagens íntimas não consentida não consentida".

Um percentual significativo estava sob segredo de justiça (43,2%), impedindo que se verificasse a natureza das partes autoras e rés. Os demais casos estavam distribuídos da seguinte forma: em 37,8% dos casos, foi iniciada por pessoas físicas, seguida por 16,2% dos casos apresentados por pessoas jurídicas e apenas 2,7% dos casos envolvendo ambos. A grande maioria dos casos (89,2%) não envolveu autores menores de idade.

Na posição de parte ré, o Google figura em 40,4% dos casos, seguida pelo Facebook em 25,5%. Outras entidades corporativas como Yahoo, Mercado Livre, Terra, Microsoft, NET e Oi foram mencionadas em alguns casos.

Em geral, são propostas ações com pedidos cumulados, sendo os mais comuns a obrigação de fazer cumulada com indenização por danos morais (32,4%) e obrigação de fazer cumulada com indenização por danos morais e materiais (16,2%). Na análise do tipo de ação com contagem isolada, foi identificado que as ações de "Obrigação de fazer" são as mais comuns, com 35 menções (59, 3%). As ações por "Indenização por

danos morais" aparecem 16 vezes (27,1%), enquanto as por "Indenização por danos morais e materiais" são contabilizadas em sete ocasiões (11,9%). Há apenas um caso (1,7%) de "Obrigação de não fazer".

Em relação aos pedidos de forma isolada, a pesquisa levantou os seguintes dados: retirada de conteúdo com 30 ocorrências (42,9%), "indenização" com 20 casos (28,6%) e "fornecimento de informação de dados sobre usuários/visitantes" com 18 casos (27,1%), "desindexação" com apenas um caso (1,4%).

Na análise dos pedidos, observa-se a frequência de mais de um fundamento para os pedidos. Porém, ao analisar de forma isolada, verifica-se o destaque para os fundamentos do dano à honra com 19 casos (39,6%), do dano à imagem com 10 casos (20,8%), disseminação não consentida de imagens íntimas com oito casos (16,7%). Os demais casos têm uma representação isolada de menos de 10%: três casos de discurso de ódio (6,3%), e casos de direitos autorais (6,3%), dois casos de fake news (4,2%), um caso de concorrência desleal (2,1%) e um caso de direito ao esquecimento (2,1%).

A análise dos dispositivos do Marco Civil da Internet, citados nas decisões judiciais, revela que o art. 19 é o mais frequentemente mencionado, com 30 ocorrências. Já o art. 5º, que trata de aspectos conceituais sobre internet, aplicações de internet, entre outros, apresenta 16 ocorrências. O art. 21, que trata da responsabilidade subsidiária dos provedores, aparece em 11 menções. Os demais dispositivos aparecem em menos de 10% dos casos.

Entre os casos analisados, 14 versam sobre ações de obrigação de fazer que estão assim distribuídas: seis apresentam pedidos de retirada de conteúdo e fornecimento de informação de dados sobre usuários e visitantes; quatro apresentam pedidos de fornecimento de informação de dados sobre usuários e visitantes; quatro tratam da retirada de conteúdo.

Os 13 casos que versam sobre as ações de obrigação de fazer, cumuladas com indenização por danos morais, estão assim distribuídos: nove casos apresentam pedidos de retirada de conteúdo e indenização; quatro casos apresentam pedidos de fornecimento de informações sobre usuários e visitantes, retirada de conteúdo e indenização.

Os sete casos versam sobre as ações de obrigação de fazer, cumuladas com indenização por danos morais e materiais, estão distribuídos da seguinte forma: três pedidos de retirada de conteúdo e indenização; um pedido de retirada de conteúdo, fornecimento de informações sobre usuários e visitantes e indenização; três pedidos de retirada de conteúdo, fornecimento de informações sobre usuários e visitantes, indenização e desindexação.

Apenas dois casos versam exclusivamente sobre ações de indenização por danos morais e um caso trata unicamente de ações de obrigação de fazer cumulada obrigação de não fazer.

A análise qualitativa dos julgados permitiu identificar as seguintes teses atualmente vigentes no STJ sobre a moderação de conteúdo.

1) Veiculação de fotografias de nudez

Por maioria, a Terceira Turma do STJ entendeu que o art. 21 do MCI tem aplicação restrita a materiais contendo cenas de imagens íntimas não consentidas ou atos sexuais de caráter privado, na qual não se enquadram, em sua ótica, a publicação de imagens íntimas não consentida produzidas para fins comerciais. Isso ocorre mesmo na hipótese de essas serem publicadas por terceiros não autorizados pela retratada e em sites diversos, daqueles para os quais as fotografias foram cedidas. O art. 21 do MCI exigiria que o conteúdo íntimo, divulgado sem autorização, fosse produzido em "caráter privado". Dessa forma, tem o objetivo de proteger e impedir a disponibilização, na rede mundial de computadores, de conteúdo íntimo produzido em caráter privado, sem a autorização da pessoa reproduzida, independentemente da motivação do agente infrator. Desse modo, não é a divulgação não autorizada de todo e qualquer material de imagens íntimas sem consentimento ou de conteúdo sexual que atrairia a regra do art. 21 do MCI, mas somente a que apresenta, intrinsecamente, uma natureza privada.

No caso de ensaios fotográficos de conteúdo íntimo que tenham sido produzidos comercialmente e divulgados por terceiros sem a autorização, a lesão a ser reparada é de cunho primordialmente patrimonial e, apenas indiretamente, a intimidade.

A tese divergente sustentava pela aplicação do art. 21 do MCI às situações do caso, por entenderem que o referido dispositivo legal se aplica não apenas à pornografia de vingança, mas também à divulgação de imagens íntimas não consentidas por guardar estreita relação com o direito à imagem, à intimidade e à privacidade assegurados no plano constitucional (art. 5o, X, da CF/88) e infraconstitucional (arts. 20 e 21 do CC/02).

2) Prestação de informações para identificação do autor do ato ilícito

É entendimento consagrado no STJ que há o reconhecimento da obrigação do provedor de conexão e acesso à internet que, uma vez instados pelo Poder Judiciário, devem fornecer, com base no endereço de IP ("Internet Protocol"), os dados cadastrais do usuário autor do ato ilícito, sendo possível a imposição de multa no caso de descumprimento da ordem. Tal obrigação se mantém, mesmo que as empresas de internet não tenham integrado a relação jurídico-processual, pois decorre do próprio dever legal da guarda, nos termos dos arts. 10, § 1º, e 22 da Lei n. 12.956/2014. Nesse contexto, havendo indícios de ilicitude e em se tratando de pedido específico voltado à obtenção dos dados cadastrais (como nome, endereço, RG e CPF) dos usuários cuja remoção já tenha sido determinada – a partir dos IPs já apresentados pelo provedor de aplicação –, a privacidade do usuário não prevalece, viabilizando o requerimento para a identificação dele.

3) Litisconsórcio entre provedor e autor do ato ilícito

A responsabilidade dos provedores de aplicações por conteúdos gerados por terceiros é subjetiva, e somente haverá solidariedade com aquele que gerou o conteúdo ofensivo se, a partir do conhecimento da lesão que determinada informação causa, o provedor não tomar as providências necessárias para a remoção.

Tratando-se de demanda na qual se busca impor ao provedor de aplicação a obrigação de remover determinadas publicações e fornecer registros de acesso e conexão, não há litisconsórcio passivo, necessário com o autor dos conteúdos. Tais providências incumbem ao provedor, mantenedor da rede social. Ou seja, eventual procedência dos pedidos não atingirá a esfera jurídica do autor das publicações.

4) Proteção integral à criança e ao adolescente

Por maioria, a Quarta Turma do STJ entendeu que, no caso de publicação de mensagem ofensiva, com insinuação sobre crime de pedofilia e imagem de menor de idade com o genitor, o provedor de aplicação, após notificado, deverá remover a publicação. O Estatuto da Criança e do Adolescente (ECA) (art. 18) e a Constituição Federal (art. 227) impõem, como dever de toda a sociedade, zelar pela dignidade da criança e do adolescente, colocando-os a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. Assim, para atender ao princípio da proteção integral consagrado no direito infantojuvenil, é dever do provedor de aplicação, na rede mundial de computadores (Internet), proceder a retirada de conteúdo envolvendo menor de idade – relacionado à acusação de que o genitor havia praticado crimes de natureza sexual – logo após ser formalmente comunicado da publicação ofensiva, independentemente de ordem judicial. Em razão da prevalência das normas de proteção da criança e do adolescente sobre a legislação protetiva da informação telemática, há prática de ato ilícito por parte do provedor de aplicações de hospedagem que, ao não excluir a imagem do menor de idade, publicada sem a autorização dos responsáveis, é relacionada a conteúdo inapropriado.

5) Vigência da lei - aplicabilidade

A jurisprudência do Superior Tribunal de Justiça (STJ) define que, para fatos anteriores à publicação do Marco Civil da Internet, basta a ciência inequívoca do conteúdo ofensivo pelo provedor, sem a retirada em prazo razoável, para que esse se torne responsável. Já após a entrada em vigor da Lei no 12.965/2014, o termo inicial da responsabilidade solidária do provedor é o momento da notificação judicial, que ordena a retirada do conteúdo da internet.

6) Individualização da URLS - Requisitos de validade da ordem judicial

Os provedores de pesquisa virtual não podem ser obrigados a eliminar do próprio sistema os resultados derivados da busca de determinado termo ou determinada expressão, tampouco os resultados que apontem uma foto ou um texto específicos, independentemente da indicação do URL da página em que esse estiver inserido. Eventual responsabilidade dos provedores por conteúdo gerado por terceiros exige, em virtude da necessidade de se permitir a localização inequívoca do material ao provedor de aplicação (a quem dirigida a ordem judicial), a indicação do URL da página ou link a ser por ele eventualmente excluído.

3.3.3.2 Brasil: Temas de Repercussão Geral 533 e 987

O Supremo Tribunal Federal analisou a constitucionalidade do art. 19 do Marco Civil da Internet (Lei nº 12.965/2014), no âmbito dos Recursos Extraordinários nº 1.037.396/SP (Tema 987) e nº 1.057.258/RJ (Tema 533), ambos com repercussão geral reconhecida.

Como adiantado no tópico 3.1 deste estudo, o Tema 533 tem origem em um caso envolvendo o Google e a extinta rede social Orkut: na ocasião, uma professora de escola pública em Belo Horizonte buscou a remoção de uma comunidade ofensiva intitulada "Eu odeio a Aliandra", além da reparação por danos morais. O Tribunal de origem considerou que haveria responsabilidade objetiva da plataforma, com base no art. 14 do Código de Defesa do Consumidor (CDC), independentemente de ordem judicial prévia. Dessa forma, o tema discute o "dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário" (Supremo Tribunal Federal, 2025b).

O Tema 987, por sua vez, discute a responsabilidade do Facebook diante da criação de um perfil falso utilizando indevidamente nome e imagem de uma usuária. A decisão da 2ª Turma Recursal Cível de Piracicaba/SP, proferida em 2017 determinou que a exigência de ordem judicial prévia configuraria restrição desproporcional ao direito à reparação por danos à personalidade. Assim, o tema refere-se à "discussão sobre a constitucionalidade do art. 19 da Lei n. 12.965/2014 (Marco Civil da Internet), que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros" (Supremo Tribunal Federal, 2025a).

Ambos os casos ilustram o cerne da controvérsia em torno do art. 19: a sua opção legislativa por um modelo de responsabilidade condicionada, em que a responsabilização civil do provedor só ocorre em caso de descumprimento de ordem judicial específica que determine a remoção do conteúdo ilícito. A exigência de prévia decisão judicial, concebida originalmente como um mecanismo de proteção à liberdade de expressão, passou a ser criticada por sua alegada morosidade e ineficácia frente à dinâmica dos fluxos informacionais nas redes sociais e outras plataformas digitais. Em resposta a esse contexto, o STF realizou, em março de 2023, uma audiência pública com ampla participação de entidades da sociedade civil, especialistas, representantes do setor e órgãos públicos.

No julgamento, o relator, ministro Dias Toffoli, apresentou voto pela declaração de inconstitucionalidade do art. 19, argumentando que o dispositivo consagra uma forma indevida de imunidade civil para os intermediários digitais, ao condicionar a responsabilidade à prévia manifestação judicial, mesmo diante de violações manifestas e continuadas a direitos fundamentais. O relator propôs, como solução, um modelo de responsabilidade extrajudicial baseado na analogia com o art. 21 do próprio MCI, que atualmente disciplina a remoção de conteúdos íntimos não consentidos mediante notificação direta da vítima.

Em voto parcialmente divergente, o ministro Luís Roberto Barroso defendeu uma solução intermediária. Propôs a adoção de um modelo dual: de um lado, a responsabilização por inércia frente a notificações extrajudiciais devidamente fundamentadas em casos de conteúdo manifestamente ilícito, excluindo-se, contudo, as situações que envolvam maior subjetividade jurídica, como as ofensas à honra; de outro, a exigência de ordem judicial prévia para os casos juridicamente mais complexos. Além disso, Barroso sugeriu que plataformas de grande porte, especialmente aquelas classificadas como "*Very Large Online Platforms*" (VLOPs), sejam submetidas a um dever de cuidado (duty of care), em linha com o regime europeu instituído pelo Digital Services Act (DSA) (Angelo, 2024).

Em 25 de junho, o plenário do STF teve mais dois votos – da ministra Cármen Lúcia e do ministro Edson Fachin – pela inconstitucionalidade (total ou parcial) do art. 19, formando maioria. Houve fixação de tese de repercussão geral, no sentido de que a exigência de descumprimento de ordem judicial específica para que os provedores de aplicações de internet sejam responsabilizados civilmente por danos causados por conteúdo publicado por terceiros já não é suficiente para proteger direitos fundamentais e a democracia (Supremo Tribunal Federal, 2025). A tese da repercussão geral será discutida com maiores detalhes a seguir.

3.3.3.3 Estados Unidos

A crescente difusão de conteúdos ilícitos pelas plataformas digitais gerou a judicialização dos conflitos com a discussão dos limites do Seção 230 do *Communications Decency Act* (CDA). O debate chegou à Suprema Corte Americana. Nos casos Gonzalez v. Google LLC (2023) e *Twitter Inc. v. Taamneh* (2023), apreciados pela Suprema Corte Americana, no qual houve a discussão sobre a responsabilidade das plataformas digitais pelo conteúdo de terceiros. Em maio de 2023, a Suprema Corte negou provimento aos pedidos indenizatórios contra as empresas de tecnologia, com a manutenção da isenção de responsabilidade, conferida pela Seção 230 do CDA às plataformas digitais, de modo que permanecem não civilmente responsáveis pelo conteúdo veiculado por terceiros.

3.3.4 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.3.4.1 Marco Civil da Internet

Como exposto no item 3.1, o Marco Civil da Internet (Lei nº 12.965/2014) constitui o principal instrumento normativo que disciplina o uso da internet no ordenamento jurídico brasileiro. Particularmente no que tange à responsabilidade civil dos provedores de aplicações de internet – plataformas digitais –, o art. 19 do Marco Civil da Internet adota um modelo de responsabilidade condicionada. De acordo com o regime estabelecido pela Lei, a plataforma somente poderá ser responsabilizada civilmente por danos decorrentes de conteúdo gerado por terceiros caso deixe de cumprir uma ordem judicial específica que determine a remoção do conteúdo considerado ilícito.

Porém, a suficiência desse regime de responsabilidade vem sendo questionada, em razão da complexidade crescente dos modelos de negócios digitais, que incluem redes sociais, *marketplaces* e serviços de mensagens. Uma das principais críticas se refere à limitação da obrigação de remoção de conteúdos subordinada à existência de ordem judicial, considerada insuficiente para conter a disseminação de conteúdos ilícitos ou prejudiciais, sendo necessário, em certos contextos, um posicionamento mais proativo por parte dos intermediários digitais, com vistas à mitigação de riscos.

O próprio Marco Civil da Internet reconhece exceções ao modelo geral de responsabilidade condicionada: um exemplo paradigmático, já discutido, encontra-se no art. 21, que excepciona a regra do art. 19 ao estabelecer a responsabilidade da plataforma que, após receber notificação extrajudicial da pessoa afetada, deixar de remover conteúdos íntimos não consentidos (como imagens ou vídeos contendo nudez ou atos sexuais). Nessas hipóteses, a responsabilização independe de ordem judicial, desde que haja omissão da plataforma em adotar as providências cabíveis após o recebimento da notificação.

A despeito da previsão de exceções ao modelo geral de responsabilidade estabelecida no MCI, tem crescido a tendência de se considerar o art. 19 manifestamente insuficiente para lidar com a real dimensão dos riscos e danos associados ao ambiente digital contemporâneo. Especificamente no âmbito do julgamento dos Temas de Repercussão Geral 533 e 987, segundo o ministro Gilmar Mendes, "já não é mais suficiente para lidar com a realidade de curadoria e moderação de conteúdo promovido pelas plataformas" (Migalhas, 2025). Essa insuficiência decorreria de dois fatores principais: primeiro, a velocidade com que conteúdos nocivos se espalham e, segundo a natureza ativa das plataformas na promoção ou impulsionamento algorítmico dessas publicações.

Em votos como o do ministro Cristiano Zanin, essa visão é reforçada com a conclusão de que a exigência de ordem judicial prévia, como estabelecido no art. 19 do MCI, oferece proteção insuficiente frente aos direitos fundamentais ameaçados pela disseminação de conteúdos ilícitos. A proposta de muitos ministros é substituir o regime estritamente judicial por um modelo escalonado, que privilegie notificações extrajudiciais ou exigência de providência imediata das plataformas quando confrontadas com conteúdos manifestamente ilícitos (como discurso de ódio, terrorismo, contas inautênticas e deepfakes), o que representaria um avanço no sentido de se reconhecer que, sem esse deslocamento, os bens jurídicos mais vulneráveis estariam à mercê da "indústria da espetacularização", nos termos do voto do ministro Dias Toffoli, do lucro que a propagação de conteúdos extremos pode gerar antes que qualquer intervenção judicial ocorra.

O quadro a seguir resume a posição dos ministros do STF sobre a matéria:

Tabela 1 – Resumo do posicionamento dos ministros do STF sobre a responsabilidade das plataformas digitais por postagens de usuários no julgamento dos Temas 533 e 987

Ministro	Art. 19 é constitucional?	Ordem judicial obrigatória?	Responsabilização sem ordem?
Dias Toffoli	Não	Não, notificação extrajudicial é suficiente	Sim, inclusive com responsabilidade objetiva
Luiz Fux	Não	Só para crimes contra a honra	Sim, quando evidente ou mediante notificação
Cristiano Zanin	Parcialmente	Sim, para casos com dúvida	Sim, para ilícitos evidentes após notificação
Luís Roberto Barroso	Parcialmente	Sim, para crimes contra a honra	Sim, para ilícitos penais evidentes
Flávio Dino	Parcialmente	Sim, para crimes contra a honra	Sim, conforme art. 21 do MCI
André Mendonça	Sim	Sim, como regra	Não, salvo exceções expressas em lei ou nos termos de uso
Gilmar Mendes	Parcialmente	Sim, para crimes contra a honra e conteúdo jornalístico	Sim, após notificação para ilícitos; sim sem notificação para impulsionamento pago; responsabilidade solidária para crimes graves se não houver remoção imediata
Alexandre de Moraes	Parcialmente	Não, nos casos de impulsionamento, contas falsas e conteúdos antidemocráticos	Sim, com dever de cuidado e responsabilidade solidária
Cármen Lúcia	Parcialmente	Sim, como regra; admite exceções diante de inércia frente a determinações legais	Sim, quando houver ataques ao Estado democrático de Direito ou descumprimento de ordens legais
Edson Fachin	Sim	Sim, como regra geral	Não há responsabilização sem ordem judicial, conforme os arts. 19 e 21 do MCI
Nunes Marques	Sim	Sim, como regra geral	Não há responsabilização sem ordem judicial, conforme os arts. 19 e 21 do MCI

Fonte: MIGALHAS. STF tem sete votos para ampliar responsabilidade de redes sociais. Migalhas, [s. l.], 2025. Disponível em: https://www.migalhas.com.br/quentes/432512/stf-tem-sete-votos-para-ampliar-responsabilidade-de-redes-sociais. Acesso em: 16 jun. 2025. (adaptado)

O Plenário do Supremo Tribunal Federal, ao julgar os Temas 533 e 987 da repercussão geral, decidiu, por 8 votos a 3, pela inconstitucionalidade parcial do art. 19 do MCI. O

STF reconheceu que a norma, como redigida atualmente, não assegura proteção suficiente a valores constitucionais relevantes, como os direitos fundamentais e a própria democracia, configurando, assim, uma omissão legislativa parcial[12]. Até que uma nova legislação seja aprovada, o dispositivo deve ser interpretado de modo a permitir a responsabilização civil dos provedores, excetuando-se os casos regulados pela legislação eleitoral e pelas normas expedidas pelo Tribunal Superior Eleitoral.

De acordo com a interpretação fixada na tese, enquanto não houver uma nova legislação sobre a matéria, o art. 19 do MCI deverá ser interpretado de modo a sujeitar os provedores de aplicação de internet à responsabilização civil, ressalvando-se a aplicação de disposições específicas de normas eleitorais. Nos termos do art. 21, as plataformas seguirão sendo responsabilizadas civilmente pelos danos decorrentes de conteúdos gerados por terceiros em casos de crime ou atos ilícitos, sem prejuízo do dever de remoção do conteúdo, lógica que se aplica também nos casos em que forem denunciadas contas falsas ou inautênticas. Já quando se tratar de crimes contra a honra, a regra do art. 19 permanece aplicável, admitindo-se, porém, a remoção do conteúdo também por meio de notificação extrajudicial. Além disso, se conteúdos ofensivos forem replicados sucessivamente após já terem sido reconhecidos como ilícitos por decisão judicial, todas as plataformas de redes sociais devem removê-los, mesmo sem nova ordem judicial, bastando que sejam notificadas judicial ou extrajudicialmente.

A decisão também estabeleceu uma "presunção de responsabilidade" para os provedores nos casos em que o conteúdo ilícito for impulsionado por anúncios pagos ou difundido por redes artificiais de distribuição, como *bots* ou IA: nessas hipóteses, a responsabilização poderá ocorrer mesmo sem notificação prévia, salvo se o provedor comprovar que agiu com diligência e em prazo razoável para tornar o conteúdo indisponível.

O STF estabeleceu ainda o dever de cuidado em caso de circulação massiva de conteúdos ilícitos graves, determinando que os provedores deverão responder civilmente quando deixarem de remover de forma imediata conteúdos que digam respeito à configuração de falha sistêmica. Tal hipótese de responsabilidade refere-se a conteúdos que configurem práticas de crimes graves previstas em rol taxativo [13]. Nesses casos,

12 A íntegra da tese encontra-se disponível em: https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/06/26205223/MCI_tesesconsensuadas.pdf. Acesso em: 2 jul. 2025.

13 "5. O provedor de aplicações de internet é responsável quando não promover a indisponibilização imediata de conteúdos que configurem as práticas de crimes graves previstas no seguinte rol taxativo: (a) condutas e atos antidemocráticos que se amoldem aos tipos previstos nos artigos 296, parágrafo único, 359-L, 359- M, 359-N, 359-P e 359- R do Código Penal; (b) crimes de terrorismo ou preparatórios de terrorismo, tipificados pela Lei nº 13.260/2016; (c) crimes de induzimento, instigação ou auxílio a suicídio ou a automutilação, nos termos do art. 122 do Código Penal; (d) incitação à discriminação em razão de raça, cor, etnia, religião, procedência nacional, sexualidade ou identidade de gênero (condutas homofóbicas e transfóbicas), passível de enquadramento nos arts. 20, 20-A, 20-B e 20-C da Lei nº 7.716, de 1989; (e) crimes praticados contra a mulher em razão da condição do sexo feminino, inclusive conteúdos que propagam ódio ou aversão às mulheres (Lei nº 11.340/06; Lei nº 10.446/02; Lei nº 14.192/21; CP, art. 141, § 3º; art. 146- A; art. 147, § 1º; art. 147-A; e art. 147-B do CP); (f) crimes sexuais contra pessoas vulneráveis, pornografia infantil e crimes graves contra crianças e adolescentes, nos termos dos arts. 217-A, 218, 218-A, 218-B, 218-C, do Código Penal e dos arts. 240, 241-A, 241- C, 241-D do Estatuto da Criança e do Adolescente; g) tráfico de pessoas (CP, art. 149-A)."

entende-se haver uma falha sistêmica, imputável ao provedor de aplicações, quando este deixar de tomar adequadas medidas de prevenção ou remoção dos conteúdos ilícitos listados, configurando descumprimento do dever de atuar de forma responsável, transparente e cautelosa. Nos termos da decisão, as medidas esperadas por parte das plataformas devem seguir o "estado da técnica", oferecendo o maior grau possível de segurança, conforme a natureza da atividade desenvolvida – embora os parâmetros para definição de "estado da técnica" não tenham sido estabelecidos. Por outro lado, ainda segundo a decisão, a existência isolada de conteúdo ilícito não configuraria, por si só, uma falha sistêmica. Já nas hipóteses em que o conteúdo removido for restabelecido por decisão judicial, não será imposta indenização ao provedor.

O STF definiu também que o art. 19 do Marco Civil permanece plenamente aplicável a plataformas específicas, como provedores de serviços de e-mail; provedores de aplicações cuja finalidade primordial seja a realização de reuniões fechadas por vídeo ou voz; e provedores de serviços de mensageria instantânea/privada exclusivamente no que diz respeito às comunicações interpessoais, resguardadas pelo sigilo das comunicações (art. 5º, inciso XIII da CF/88). Já em relação aos *marketplaces*, a tese estabeleceu que se trata de plataformas sujeitas às normas do Código de Defesa do Consumidor, sendo, portanto, responsabilizadas conforme o regime consumerista.

Além disso, deveres adicionais foram fixados. Os provedores de aplicações de internet passam a ter o dever de instituir mecanismos de autorregulação que, de forma obrigatória, incluam sistemas de notificação, garantias mínimas de contraditório e ampla defesa, bem como a elaboração de relatórios anuais de transparência que abranjam notificações extrajudiciais, anúncios publicitários e conteúdos impulsionados. Além disso, deverão oferecer canais específicos de atendimento — preferencialmente eletrônicos — acessíveis tanto a usuários quanto a não usuários, os quais devem estar permanentemente disponíveis e amplamente divulgados nas plataformas. Tais regras deverão ser publicadas de forma transparente e acessível ao público e periodicamente revisadas.

Exige-se ainda que os provedores que operam no Brasil mantenham sede e representação formal no território nacional, sendo esta exercida por pessoa jurídica devidamente identificada, cuja razão social e meios de contato deverão estar facilmente disponíveis nos respectivos sites. O representante legal deverá estar investido de plenos poderes para atuar administrativa e judicialmente, prestar às autoridades informações sobre o funcionamento da plataforma, suas práticas de moderação de conteúdo e gestão de reclamações, além dos relatórios de transparência, das estratégias de mitigação de riscos sistêmicos, das políticas de perfilamento de usuários, da veiculação de anúncios e do impulsionamento de conteúdo. Nos termos da tese, caberá ainda ao representante cumprir ordens judiciais e assumir eventuais sanções, penalidades financeiras ou obrigações legais decorrentes de descumprimento normativo.

No que tange à natureza da responsabilidade civil dos provedores de conteúdo publicados por terceiros, a tese afastou a incidência de responsabilidade objetiva. Em relação

à modulação dos efeitos temporais da decisão, a fim de preservar a segurança jurídica, estabeleceu-se que a decisão somente se aplicará prospectivamente, ressalvadas decisões transitadas em julgado.

Finalmente, na tese enunciada, faz-se um apelo ao Congresso Nacional, a fim de que "seja elaborada legislação capaz de sanar as deficiências do atual regime quanto à proteção de direitos fundamentais" na Internet.

3.3.4.2 Código de Defesa do Consumidor

No ordenamento jurídico brasileiro, a Lei nº. 8.078/90 (Código de Defesa do Consumidor – CDC) atua como um dos principais instrumentos normativos para a regulação dos consumidores no ambiente digital. O CDC disciplina, de forma ampla, as relações de consumo e estabelecendo padrões de conduta, responsabilidade e informação a serem observados por todos os fornecedores, inclusive aqueles que operam no meio digital.

A responsabilidade das plataformas de comércio eletrônico, particularmente os *marketplaces*, tem sido objeto de especial atenção por parte da doutrina e da jurisprudência nacional. O art. 14 do CDC consagra a responsabilidade objetiva dos fornecedores de serviços, determinando que respondem, independentemente de culpa, pelos danos causados aos consumidores em decorrência de defeitos na prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos [14]. Tal disposição tem servido de fundamento jurídico para o reconhecimento da responsabilidade solidária das plataformas pelos vícios e defeitos dos produtos comercializados por intermédio de seus ambientes virtuais.

O Superior Tribunal de Justiça, ao analisar o Recurso Especial nº 1.634.851/SP, consolidou entendimento no sentido de que as plataformas que intermediam relações de consumo devem ser consideradas integrantes da cadeia de fornecimento, atraindo, por consequência, a responsabilidade solidária pelos danos advindos da comercialização de produtos defeituosos. Na oportunidade, a Terceira Turma da Corte firmou a seguinte orientação:

14 "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§ 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I - o modo de seu fornecimento;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - a época em que foi fornecido.

§ 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.

§ 3º O fornecedor de serviços só não será responsabilizado quando provar:

I - que, tendo prestado o serviço, o defeito inexiste;

II - a culpa exclusiva do consumidor ou de terceiro.

§ 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.

> As plataformas de comércio eletrônico, ao intermediar a relação de consumo, assumem a responsabilidade solidária pelos vícios e defeitos dos produtos comercializados por meio de seu ambiente virtual, uma vez que integram a cadeia de fornecimento e se beneficiam economicamente da atividade. Tal entendimento visa a garantir a efetividade da proteção ao consumidor, conforme preceitua o artigo 14 do Código de Defesa do Consumidor.

O fundamento doutrinário dessa orientação também é sólido. Cláudia Lima Marques defende que a responsabilidade das plataformas decorre não apenas da literalidade do CDC, mas também de princípios contratuais estruturantes, como a boa-fé objetiva e a função social do contrato, asseverando:

> As plataformas digitais, ao fornecerem um ambiente propício para a realização de negócios e auferirem lucros dessa intermediação, devem responder solidariamente pelos danos causados aos consumidores. Esta responsabilidade decorre não apenas da previsão legal do CDC, mas também dos princípios da boa-fé objetiva e da função social do contrato, que impõem deveres de lealdade e transparência às empresas que atuam no mercado de consumo. (Marques, 2015, p. 203)

É importante ressaltar que a aplicabilidade do CDC não se restringe às plataformas de intermediação comercial (*marketplaces*), mas se estende, de modo geral, a todos os agentes econômicos que, por meio de suas plataformas digitais, desenvolvam atividades no âmbito das relações de consumo. Independentemente de sua natureza – seja um *marketplace*, uma rede social, um motor de busca ou qualquer outro tipo de provedor de serviço de internet – a incidência do CDC é determinada pela configuração da relação de consumo, observando-se a presença dos elementos subjetivos (consumidor e fornecedor) e objetivos (produto ou serviço) previstos na legislação consumerista.

Esse entendimento foi reafirmado pelo Superior Tribunal de Justiça no julgamento do Recurso Especial nº 1.444.008/RS, em que se discutia a responsabilidade de um provedor de buscas de produtos no comércio eletrônico. No caso, a Corte ressaltou que a incidência do CDC independe de o serviço ser gratuito e que a configuração da qualidade de fornecedor demanda a análise do grau de intermediação efetiva nas relações comercial. A decisão foi assim ementada:

> CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA VOLTADA AO COMÉRCIO ELETRÔNICO. INTERMEDIAÇÃO. AUSÊNCIA. FORNECEDOR. NÃO CONFIGURADO.
>
> 1. Ação ajuizada em 17/09/2007. Recurso especial interposto em 28/10/2013 e distribuído a este Gabinete em 26/08/2016.
>
> 2. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90.

3. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo.

4. Existência de múltiplas formas de atuação no comércio eletrônico.

5. O provedor de buscas de produtos que não realiza qualquer intermediação entre consumidor e vendedor não pode ser responsabilizado por qualquer vício da mercadoria ou inadimplemento contratual.

6. Recurso especial provido.

A doutrina nacional também tem sido enfática ao afirmar a plena incidência do CDC sobre as relações jurídicas de consumo realizadas por meio da internet, ressalvadas situações excepcionais. Nas palavras de Newton De Lucca:

> Desde as primeiras palestras que proferi sobre o tema da internet, venho afirmando que, no âmbito das relações de consumo, a aplicação da legislação consumerista às relações jurídicas de consumo celebradas por essa via é plena, conquanto isso não signifique afirmar, absolutamente, seja ela suficiente. Tirante uma ou outra situação deveras peculiar – como, por exemplo, a aquisição de produtos digitais que se incorporam, desde logo, ao patrimônio do comprador, tornando extremamente delicado, em tais hipóteses, o exercício do direito de arrependimento previsto no art. 49 do nosso Código de Defesa do Consumidor – é certo não haver diferença ontológica e axiologicamente relevante entre o que se passa no mundo real e no mundo virtual. A questão da caracterização da relação de consumo, no âmbito da internet, põe-se exatamente da mesma forma. Aplicar-se-á total ou parcialmente o CDC às relações jurídicas, dependendo de serem ou não os sujeitos atuantes nessas relações, fornecedores e consumidores. Identificados como tais, razão nenhuma existe para que lhes sejam criados óbices à plena aplicação da legislação tutelar. (De Lucca, 2003, p. 410)

Já no contexto do já mencionado julgamento do STF sobre o art. 19 do MCI, o ministro André Mendonça firmou posição favorável à aplicação estruturada do CDC junto a modelos de autorregulação das plataformas e defendeu que a responsabilização de provedores deve se pautar por "procedimentos e governança, e não por conteúdos isolados", asseverando que, caso observados protocolos de compliance, transparência e devido processo, as empresas podem "afastar a responsabilidade" por conteúdos de terceiros. No seu voto, houve a proposta de aplicação de deveres procedimentais com base no CDC, evitando responsabilização pontual e garantindo salvaguardas como a proteção da personalidade digital e da liberdade de expressão.

Por sua vez, o ministro Flávio Dino trouxe à discussão uma associação direta entre a responsabilização das plataformas e o artigo 14 do CDC, considerando falhas sistêmicas e omissões graves como base para ação civil e defendendo que "os provedores podem ser responsabilizados civilmente nos termos do artigo 14, § 1º, II, do Código de Defesa do

Consumidor, pelos conteúdos criados por terceiros" em casos de crimes contra crianças, suicídio, terrorismo ou apologia à violência. Assim, propôs a ampliação do CDC para além dos deveres de informação e segurança, impondo um dever de cuidado digital ativo e diferenciado, conforme a gravidade do conteúdo.

3.3.4.3 Projeto de Lei nº 2.630/2020

O Congresso brasileiro propôs uma rediscussão sobre o tema, de modo a tornar a regulação das atividades dessas plataformas mais atualizada aos novos debates e impactos que têm gerado na sociedade e nas instituições. O Projeto de Lei nº 2630/2020, de autoria do senador Alessandro Vieira, foi aprovado pelo Senado Federal no mesmo ano e passou a tramitar em regime de urgência. Contudo, em razão da falta de maioria na Câmara dos Deputados, a votação foi adiada. Recentemente, o presidente da Câmara dos Deputados decidiu criar um grupo de trabalho diante da impossibilidade de estabelecer um consenso em torno do PL 2630/2020.

3.3.4.4 Projeto de Lei nº 4.691/2024

O Projeto de Lei 4.691/2024, de autoria dos deputados Silas Câmara e Dani Cunha, em tramitação na Câmara dos Deputados, dispõe sobre o direito e a garantia fundamental à livre manifestação do pensamento na internet, o livre exercício da atividade econômica na internet, a organização e funcionamento das plataformas, serviços e mercados digitais na internet e dá outras providências.

Ao compararmos este projeto com o PL nº 2.630/2020, verificamos que o texto indica um índice de sobreposição textual inferior a 5%, o que evidencia que a maior parte do conteúdo produzido ao longo de quatro anos de debates parlamentares e audiências públicas, consolidado no parecer do deputado Orlando Silva, foi substancialmente desconsiderada pelos autores da nova proposição.

Do texto anteriormente rejeitado, o PL nº 4.691/2024 manteve, essencialmente, os dispositivos que tratam da identificação, análise e mitigação de riscos sistêmicos pelas plataformas digitais (arts. 7º e 8º). Tais dispositivos, inspirados em marcos regulatórios internacionais como o *Digital Services Act* da União Europeia, impõem aos provedores de aplicação com base algorítmica a adoção de medidas organizacionais e técnicas voltadas à mitigação proporcional e eficaz de tais riscos.

Dentre as obrigações previstas, destacam-se: (i) a necessidade de reconfiguração de serviços e interfaces; (ii) a revisão dos termos de uso e dos critérios de moderação; (iii) o aprimoramento dos fluxos de análise de conteúdo e processamento de notificações de violação; (iv) a realização de testes regulares em sistemas algorítmicos, incluindo aqueles voltados à recomendação de conteúdo e à publicidade dirigida; (v) a adoção de reforços internos em procedimentos de governança e compliance; (vi) a melhoria na transparência informacional oferecida aos usuários; e (vii) a implementação de salvaguardas adicionais para proteção dos direitos de crianças e adolescentes.

No entanto, diferentemente da proposta contida no PL nº 2.630/2020, a nova versão legislativa suprimiu as obrigações preventivas diretamente vinculadas ao chamado "dever de cuidado" (*duty of care*). No projeto original, o referido dever impunha às plataformas a obrigação de agir de ofício na identificação, moderação e eventual remoção de conteúdos envolvendo tipologias específicas de ilícitos, tais como: (i) crimes contra o Estado Democrático de Direito; (ii) atos de terrorismo e crimes correlatos; (iii) induzimento, instigação ou auxílio ao suicídio ou à automutilação; (iv) crimes envolvendo crianças e adolescentes; (v) práticas de racismo; (vi) violência contra a mulher; e (vii) infrações sanitárias cometidas durante situações de emergência em saúde pública.

3.3.5 Comentários sobre o texto do projeto da reforma do Código Civil

A reforma do Código Civil reconhece que, mesmo quando o serviço é gratuito para o usuário ou por ele não remunerado, a atenção e audiência desse são transformadas em mercadorias e integram o complexo de bens empresariais, fenômeno estudado no cerne da economia da atenção (Davenport; Beck, 2001). Passa a existir a compreensão sobre a posição oblíqua do usuário na relação jurídica entre a plataforma digital e um terceiro, relação essa da qual o usuário não participa formalmente como sujeito contratante e a contraprestação econômica não é diretamente dele exigida. Não obstante, é a atenção e audiência do usuário (com ou sem a inclusão dos seus dados pessoais) que permitem, muitas vezes, a monetização da plataforma digital por um terceiro, interessado na audiência mantida pelo ambiente digital e realização da publicidade naquela oportunidade difusa. A vantagem da ambiência digital decorre da ubiquidade[15] da interação com o usuário, não mais dependente de um ponto comercial ou uma localização geográfica para acessar o usuário.

É justamente nesse contexto econômico que foi percebida a necessidade de que as práticas mercantis, como a publicidade persuasiva e os sistemas recomendatórios, alimentados por algoritmos, e interações no ambiente digital fossem objeto de regulamentação.

Nota-se que a presença do usuário confere receitas à plataforma digital, à medida que essa direciona a publicidade de terceiros ao usuário, conforme os perfis persuasivos arquitetados pela plataforma digital para engajar o usuário a ações específicas naquele ambiente. À medida que essa plataforma é hábil a atrair e engajar o comportamento do usuário para os escopos pretendidos, como influência para compras, processos eleitorais etc., amplia-se o valor agregado da plataforma digital. Quanto maior o número de usuários, maior é a audiência do ambiente digital a ser monetizada. Quanto maior é o engajamento dos usuários, maior é o valor agregado da plataforma e a potencialidade de lucratividade naquele ambiente.[16]

---

15 Sobre a ubiquidade da tecnologia, cf., entre outros, FOGG, B. J. *Persuasive technology: using computers to change what we think and do (interactive technologies)*. Morgan Kaufmann, 2002.

16 Sobre o poder das plataformas digitais, cf., entre outros, GILLESPIE, Tarleton. *The politics of 'platforms'*. New Media & Society. V. 12. N. 3, 2010. 347-364p. FLORIDI, Luciano. *The onlife manifesto: being a human in a hiperconnected era. Springer*, 2014.

O projeto de reforma do Código Civil introduz, em sede de interpretação autêntica, os conceitos de (i) ambiente digital; (ii) plataforma on-line; (iii) plataforma digital de grande alcance; e, ainda, (iv) novos direitos da personalidade e situações jurídicas no ambiente digital. Conceitos esses que são fundamentais para a compreensão sistemática da regulamentação das plataformas digitais, que deve ser feita à luz do seu eixo axiológico.

Nessa linha, segundo o próprio texto da reforma, o ambiente digital é considerado o espaço virtual interconectado por meio da internet, compreendendo redes de computadores, dispositivos móveis, plataformas digitais e quaisquer tecnologias interativas. Plataforma digital é, por sua vez, considerado pelo legislador como espécie de espaço virtual, no qual sobreleva-se a hospedagem digital e a funcionalidade de armazenamento e a difusão de informações ao público. O ambiente virtual é gênero de espaço virtual, do qual a plataforma digital é apenas uma espécie.

Entre as espécies de plataformas digitais, houve a expressa conceituação das plataformas digitais de grande alcance que denotam os serviços de hospedagem digital. A essas plataformas massivas, o legislador destinou regulamentação mais específica e protetiva, com encaminhamento semelhante à *Digital Service Act*, da União Europeia.

Para a ambiência digital e o ecossistema de produtos e serviços, suscetíveis de oferta em quaisquer tecnologias digitais, o texto da reforma prevê o pleno exercício da liberdade de informação e reafirma a autonomia individual no ambiente digital, sopesados à regulação dos serviços digitais. Estabelece, como parâmetros interpretativos expressos da interpretação dos fatos, atos, negócios e outras atividades civis que tiverem lugar no ambiente digital: a dignidade humana, a inclusão, acessibilidade, igualdade, eticidade, proteção à infância e adolescência e segurança contra investidas que possam interferir no discernimento, mesmo momentaneamente. Destaca-se, neste último, a proteção da liberdade cognitiva, essencial à plena autonomia da vontade. Houve uma nova repersonalização do direito privado e reumanização em face do ambiente digital.

Nessa perspectiva, as alterações propostas no projeto de reforma do Código Civil no tocante às plataformas digitais estruturam-se em seis eixos:

(i) A indicação de uma base principiológica que assegure um ambiente digital seguro;

(ii) A previsão de medidas de diligência e de regras para moderação de conteúdo;

(iii) O estabelecimento de um sistema de responsabilidade civil das plataformas digitais;

(iv) A previsão de critérios de acessibilidade e transparência na elaboração dos termos de uso das plataformas digitais, com a imposição de nulidade absoluta para as previsões contrárias às normas cogentes ou de ordem pública;

(v) A exigência de identificação, análise e avaliação anual dos riscos sistêmicos pelas plataformas digitais de grande alcance, derivados da arquitetura do ambiente digital e do funcionamento dos serviços, considerando os riscos de difusão de conteúdo ilícito e os

possíveis efeitos (reais ou previsíveis) sobre os direitos da personalidade, os processos eleitorais, o discurso cívico, a segurança pública e a saúde pública. Na avaliação de risco, essas plataformas deverão considerar concepção dos próprios sistemas algorítmicos, os sistemas de moderação de conteúdo, os termos e políticas de uso, bem como os sistemas de seleção e exibição de anúncios publicitários;

(vi) A implementação de auditoria independente e periódica, com frequência anual, nas plataformas digitais de grande alcance, às custas da empresa, para verificar a conformidade com as obrigações estabelecidas no novo texto normativo.

A reforma do Código Civil brasileiro introduz profundas inovações na regulamentação das plataformas digitais, antes mais restrita ao Marco Civil da Internet e à LGPD, bem como às cláusulas gerais sobre invalidades e responsabilidade civil do diploma civilista.

Além disso, estabelece os seguintes princípios a fim de assegurar um ambiente digital seguro e confiável: transparência, boa-fé, função social e prevenção de danos. Conservam-se os princípios estruturantes da boa-fé objetiva, socialidade e operabilidade, que informam e condicionam a eticidade dos atos e das atividades dos usuários e provedores no ambiente digital, inaugurando, todavia, novos deveres anexos.

Essa regulamentação marca um avanço no direito privado, ampliando a função protetiva da área e adaptando-se às novas realidades tecnológicas e aos meios de interação social.

A reforma do Código Civil brasileiro, ao abordar as plataformas digitais sob a perspectiva dos impactos individuais e difusos no seio social, reafirma a centralidade axiológica da pessoa humana e o respeito aos direitos da coletividade de usuários. A regulamentação da tecnologia digital pode ser, nessa linha de raciocínio, percebida enquanto instrumento de empoderamento do indivíduo e dos mais vulneráveis no âmbito digital, bem como, sob o prisma coletivo, um instrumento de preservação do equilíbrio nas relações jurídicas contemporâneas e de proteção sustentável do meio ambiente e do ecossistema digital.

No tocante às plataformas digitais[17], foram introduzidas exigências inéditas, como deveres correlatos ou anexos aos princípios aplicáveis ao ambiente digital, como: (i) acessibilidade, transparência e fácil compreensão aos termos contratuais de uso das plataformas e demais políticas digitais; (ii) a realização de auditorias independentes, custeadas pelas plataformas digitais; e (iii) a avaliação de riscos sistêmicos.

Os dois últimos deveres recaem exclusivamente sobre as plataformas digitais de grande alcance [18]. Evidencia-se, com isso, a tentativa do legislador brasileiro de harmonizar a proteção da pessoa humana dada a inovação tecnológica com a proteção da liberdade econômica e dos novos negócios empresariais digitais, a partir de uma análise autêntica

17 Plataforma digital on-line, em interpretação autêntica do legislador, é conceito assim introduzido no novo texto: "art. 2.027-G. Consideram-se como plataforma on-line os serviços de hospedagem virtual que tenham como funcionalidade principal o armazenamento e a difusão de informações ao público".

18 Plataforma digital de grande alcance, em interpretação autêntica do legislador, é conceito assim introduzido no novo texto: "art. 2.027-H. Consideram-se como plataforma digital de grande alcance os serviços de hospedagem virtual que tenham como funcionalidade principal o armazenamento e a difusão de informações ao público, cujo número médio de usuários mensais no Brasil seja superior a 10 milhões, tais como as redes sociais, as ferramentas de busca e os provedores de mensagens instantâneas".

da dimensão dos riscos regulatórios e considerando a intervenção subsidiária e excepcional Estado sobre as atividades econômicas (art. 2º, III, da Lei nº. 13.874/19).

O projeto de reforma mantém a tutela protetiva de viés existencialista, mas introduz disposições inéditas que se relacionam concretamente à arquitetura e ao funcionamento das plataformas digitais. Essas inovações abrangem aspectos como (i) a concepção e funcionamento de sistemas algorítmicos, (ii) mecanismos de curadoria e moderação de conteúdo, (iii) termos e políticas de uso, (iv) critérios de seleção e exibição de publicidade, (v) a automatização de processos e formação de perfis de usuários e (vi) informação sobre monetização da plataforma e anúncios publicitários.

De forma inédita, a reforma do Código Civil estabelece deveres colaterais de natureza protetiva social e difusa, voltados à preservação do ambiente digital enquanto espaço de interação social e coletiva não geográfico. Nesse espaço virtual, a interação e o ambiente de negócios devem observar parâmetros normativos e éticos. Esses deveres transcendem a relação contratual tradicional e refletem uma preocupação com a higidez das interações sociais e econômicas mediadas pelas plataformas, não restritas às relações intersubjetivas.

Valendo-se da expressão de Peter Häberle (1997), poder-se-ia falar, por analogia, em uma sociedade aberta de intérpretes digitais. A arquitetura digital envolve, além do uso individual, a coleta de dados massivos dos usuários, ainda que anonimizados. E, com isso, potencializa a capacidade de influência difusa da plataforma digital, enquanto agente econômico, no auditório dos usuários, acolhidos coletivamente no ambiente digital.

Daí a exigência de transparência, decorrente da própria opacidade do meio digital, e a necessidade de operacionalizar uma sociedade digital aberta, que possa realizar o escrutínio da adequada normatividade das plataformas digitais. Essa sociedade é a verdadeira afetada pelas práticas digitais, de modo que possa se manifestar e influenciar legitimamente sobre o *design* digital para além da mera adesão aos termos de uso.

Entre os novos deveres, considerando as especificidades da ambiência digital nas esferas individual e coletiva, destacam-se obrigações que não se relacionam aos indivíduos. Nesse sentido, é possível mencionar o fato de que os termos de uso são individualmente acordados, mas os efeitos relacionam-se difusamente à comunidade ou ao auditório de usuários, pois a falta de autodeterminação informativa e liberdade cognitiva individual degradam o próprio ambiente digital. A partir da reforma, prevê-se:

1. A obrigatoriedade de auditorias independentes para verificar a conformidade das plataformas com os princípios de transparência, boa-fé e demais previsões sobre os direitos da pessoa na plataforma e sobre o meio ambiente digital;

2. A análise de riscos sistêmicos associados ao impacto das operações digitais no ambiente social e econômico;

3. A inclusão de políticas voltadas à proteção coletiva dos usuários e à garantia de um ecossistema digital sustentável, com a adequada alocação de riscos entre os usuários e as grandes empresas de tecnologia.

O texto da reforma estabelece que os termos de uso das plataformas digitais devem ser redigidos de forma acessível, intuitiva e transparente, determinando a nulidade de pleno direito das cláusulas contratuais que estejam em desconformidade com as normas cogentes ou de ordem pública. A opção legislativa, por cominar expressamente a nulidade de pleno direito, em detrimento da mera anulabilidade por eventual vício de consentimento, suscita reflexões relevantes.

A escolha legislativa por cominar nulidade de pleno direito[19] demonstra um esforço normativo no sentido de reforçar a proteção jurídica do usuário, afastando a necessidade de comprovação do vício ou prejuízo individual para a invalidação da cláusula. Essa postura visa garantir uma maior efetividade às normas de ordem pública e às diretrizes protetivas da pessoa humana e do meio ambiente digital. O ecossistema digital enfrenta a assimetria informacional e a má alocação de riscos entre provedores e usuários, camuflados, muitas vezes, nos códigos formais e nas interfaces digitais, que são armadilhas para o usuário e prejudiciais à higidez do ecossistema digital.

A escolha da cominação expressa de nulidade é, acima de tudo, simbólica no novo texto. Nos casos de violação de normas cogentes e indisponíveis, declarar-se-á a nulidade de pleno direito, na forma do art.166 do Código Civil, atraindo-se o panorama protetivo típico da nulidade, cognoscível de ofício e insuscetível de confirmação ou convalidação.

À medida que as plataformas digitais se caracterizam como um meio ambiente, cuja lisura deve ser protegida, há um forte caráter publicístico[20] na arquitetura dessas plataformas, instituído em razão da comunidade de pessoas que participam do ambiente. Nessas hipóteses, os interesses coletivos ou difusos – da comunidade – não são transacionáveis.

Nota-se, portanto, que os termos de uso das plataformas digitais devem ser de fácil compreensão ao usuário, mas também devem observar a normas imperativas, em proteção ao ecossistema digital e à comunidade. Há que se frisar que, nessa previsão normativa, estão presentes notas individuais, típicas dos negócios jurídicos bilaterais e sinalagmáticos, como também há nuances protetivas de direito público e difuso para manter a higidez do ambiente digital, ainda que sem prejuízos individuais. Nesse contexto, é cominada a nulidade de pleno direito aos termos de uso das plataformas digitais que contrariarem as normas cogentes ou de ordem pública.

Andou bem, portanto, o legislador da reforma do Código Civil em prever e costurar legislativamente, na regulamentação das plataformas digitais, a possibilidade de reconhecimento da nulidade de pleno direito, atrelado ao *disclosure* dos riscos sistêmicos para as plataformas de grande alcance e aliado à realização de auditorias independentes.

19 Sobre a teoria do fato jurídico e invalidades, cf. MELLO, Marcos Bernardes de. *Teoria do fato jurídico: plano da existência*. 20 ed. São Paulo: Saraiva, 2014. p. 312.

20 Sobre o ilícito nulificante, cf. PONTES DE MIRANDA, Francisco Cavalcante. *Tratado de Direito Privado*. São Paulo: RT, 2013.

O legislador, ao estabelecer como exigência protetiva o dever contratual de revelação dos riscos sistêmicos na plataforma digital de grande alcance, considerou devidamente a baixa cognição e opacidade da esfera digital de natureza difusa, ainda que os termos de uso contratuais individuais sejam claros e precisos, logrando o consentimento individual.

Importa destacar que não seria suficiente a mera cominação de nulidade de pleno direito aos termos de uso da plataforma que fossem contrários às normas cogentes. A declaração de nulidade pressupõe a antecedente transparência sobre as práticas digitais. Ocorre que as plataformas digitais padecem, justamente, da opacidade e falta de referibilidade normativa, impondo-se, *quid pro quo*, a revelação de riscos sistêmicos e auditoria do design digital como critério de confiabilidade e conformidade normativa.

As práticas de gerenciamento de informações em plataformas digitais envolvem ferramentas de moderação de conteúdo que podem abranger a desindexação e a exclusão de conteúdo, já abordadas no item 3.1. Porém, os instrumentos de moderação de conteúdo vão além dessas possibilidades e envolvem também a aplicação de advertências, suspensão de contas e até a criação de canais de denúncias para que os usuários possam reportar os conteúdos infringentes.

Inicialmente, a moderação de conteúdo nas plataformas digitais, em especial nas redes sociais, era uma prática secundária. Conforme essas plataformas foram se expandindo, a moderação de conteúdo passou a ter um papel central já que os conteúdos compartilhados podem envolver racismo, misoginia, discursos de ódios, além de outras formas de manifestação ilegais.

Por sua importância na sociedade, a moderação de conteúdo é indispensável quando se trata de um devido processo informacional condizente com um Estado Democrático de Direito. No Brasil, o Marco Civil da Internet (MCI), estabelecido pela Lei nº 12.965/2014, regula a moderação de conteúdo, estabelecendo a responsabilidade dos provedores de internet e das aplicações no que diz respeito a conteúdos gerados por terceiros. O art. 18 do MCI estabelece que o provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. Tal responsabilidade só emergirá, nos termos do artigo 19 do MCI, se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e no prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

A ordem judicial deverá ter a identificação clara e específica do conteúdo apontado como infringente. Haverá responsabilidade subsidiária, nos termos do art. 21 do MCI, nos casos de violação da intimidade decorrente da divulgação, sem a autorização de seus participantes, imagens, vídeos ou outros materiais contendo cenas de nudez ou atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou representante legal dele, a plataforma deixar de promover a indisponibilização desse conteúdo.

Como aponta Schreiber (2015), o MCI, em vez de regular o *notice and take down* para que não houvesse abusividade na utilização, extinguiu quase que por completo esse mecanismo. O autor destaca que o art. 19 do MCI se mostra inefetivo ao colocar em perspectiva o fato de o ordenamento já permitir, por óbvio, a judicialização de questões lesivas ao indivíduo. No entanto, ainda segundo Schreiber, o fato de se exigir ordem judicial específica para a responsabilização dos provedores deixa o lesado desprotegido e, em um movimento contraproducente, estimula que os conflitos sejam levados a um judiciário já sobrecarregado, o que prolonga o período de circulação dos conteúdos (Schreiber, 2015).

Remete-se, nessa oportunidade, às observações indicadas no item, 3.3.4.1, ao tratar da tese fixada no âmbito do julgamento dos Temas de Repercussão Geral 533 e 987.

Um cuidado inicial merece destaque: poderia haver uma interpretação superficial de que as plataformas digitais representam apenas uma transposição do meio analógico para o meio digital. No entanto, trata-se de um erro de compreensão comum. A discussão sobre as plataformas digitais transcende a mera transformação digital; não se trata apenas de transferir relações intersubjetivas, fatos, atos, negócios jurídicos, obrigações ou contratos para um ambiente digital. A arquitetura dessas plataformas envolve um rearranjo fundamental das relações jurídicas (Nunes, 2020), remetendo a um contexto de vínculos ou liames subjetivos estabelecidos primariamente no meio digital. Não é, pois, uma transposição digital, mas uma reimaginação das relações jurídicas, da governança legal e dos institutos jurídicos a partir de uma perspectiva transdisciplinar, pensada para o fenômeno digital.

Forte nessas razões e considerando o estado da arte e do desenvolvimento do ambiente digital, os dispositivos da reforma do Código Civil buscam oferecer respostas aos dilemas jurídicos-regulatórios da ambiência digital. No âmbito da reforma do Código Civil, a proposta de responsabilização das plataformas digitais é a seguinte:

> Art. 2.027-Z. As plataformas digitais podem ser responsabilizadas administrativa e civilmente:
>
> I – pela reparação dos danos causados por conteúdos gerados por terceiros cuja distribuição tenha sido realizada por meio de publicidade da plataforma;
>
> II – por danos decorrentes de conteúdos gerados por terceiros, quando houver descumprimento sistemático dos deveres e das obrigações previstas neste Código, aplicando-se o sistema de responsabilidade civil nele previsto.

Como se verifica, o PL 4/2025 estabelece que as plataformas digitais poderão ser responsabilizadas, tanto em âmbito administrativo quanto civil, em duas situações específicas. Primeiro, quando danos forem causados a partir de conteúdos gerados por terceiros que tenham sido distribuídos por meio de publicidade da própria plataforma. Segundo, no caso de haver um descumprimento sistemático dos deveres prescritos no referido Código, em que serão aplicadas as normas de responsabilidade civil definidas no Código.

Dessa forma, o texto da reforma do Código Civil se alinha a outras iniciativas que evidenciam a necessidade de revisão do sistema de responsabilidade civil atual, entre elas o Projeto de Lei 2.630/20 e as recentes discussões no Supremo Tribunal Federal (STF), notadamente no âmbito dos Temas de Repercussão Geral 533 e 987.

A proposta de reforma do Código Civil, no que tange à responsabilidade civil das plataformas, mostra-se em sintonia com a tese fixada pelo STF no julgamento do Temas 533 e 987 da repercussão geral, sobretudo no que se refere à superação da regra geral do art. 19 do Marco Civil da Internet. As novas disposições, fixadas na tese, exigem que as plataformas digitais adotem medidas diligentes para prevenir e mitigar a circulação de conteúdo ilícito (art. 2.027-V), o que corresponde diretamente ao entendimento do STF de que os provedores podem ser responsabilizados civilmente quando, cientes da ilicitude, permanecerem inertes. Por sua vez, o § 3º do art. 2.027-V, ao determinar que a plataforma deve agir diante de notificação que indique potencial ilicitude de um conteúdo, incorpora um aspecto relevante da nova interpretação estabelecida, qual seja, de que a responsabilização não depende, necessariamente, de ordem judicial, desde que haja conhecimento e omissão do conteúdo ofensivo.

A exigência de mecanismos eficazes de reclamação e reparação (§ 2º do art. 2.027-V) conecta-se diretamente à imposição, fixada pelo STF, de que plataformas mantenham canais acessíveis ao público para recebimento de notificações extrajudiciais, especialmente nos casos de conteúdos ilícitos. Já o art. 2.027-W do PL 4/2025 reforça esse entendimento, ao impor deveres de transparência sobre os instrumentos e procedimentos de moderação, principalmente se automatizados ou vinculados à monetização – elementos mencionados expressamente pelo STF ao admitir presunção de responsabilidade em situações que envolvam impulsionamento pago ou disseminação artificial por meio de *bots* e contas automatizadas.

O art. 2.027-X, por sua vez, incorpora a lógica de "falha sistêmica" mencionada expressamente na decisão do Supremo, ao estabelecer que as plataformas de grande alcance devem identificar, avaliar e mitigar riscos sistêmicos decorrentes de sua estrutura e funcionamento. Entre os riscos elencados estão a difusão de conteúdos ilícitos e os efeitos sobre direitos da personalidade, saúde pública e processos eleitorais — todas dimensões expressamente abordadas pelo STF ao reconhecer a insuficiência do regime atual para a proteção de bens jurídicos de alta relevância constitucional. O § 3º do mesmo artigo, ao exigir medidas de mitigação proporcionais ao impacto nos direitos da pessoa, aprofunda a exigência jurisprudencial de atuação responsável, cautelosa e conforme o estado da técnica.

A exigência de auditorias independentes (art. 2.027-Y) também encontra respaldo na tese do STF, pois consolida uma lógica de responsabilização preventiva e controle externo sobre práticas internas das plataformas, reforçando o dever de prestação de contas e de atuação diligente para prevenir violações sistêmicas. Finalmente, o art. 2.027-Z sin-

tetiza a proposta de um novo regime de responsabilidade civil ao prever expressamente a responsabilização por danos decorrentes da veiculação publicitária de conteúdos de terceiros e por descumprimento sistemático dos deveres legais – categorias diretamente previstas pelo STF, tanto na criação de presunções de responsabilidade quanto na caracterização da falha sistêmica como fundamento para responsabilização.

A proposta está ainda em total consonância com as tendências recentes de diversos sistemas jurídicos, que buscam revisar a responsabilidade das plataformas digitais intermediárias, considerando a capacidade delas de influenciar o fluxo de informações e as externalidades negativas. Tal tendência pode ser encontrada nas recentes decisões judiciais nos Estados Unidos, que vêm estabelecendo limites para a Seção 230 do *Communications Decency Act* (CDA), bem como no Regulamento Geral de Proteção de Dados (GDPR), que constitui um marco nessa mudança de perspectiva ao instituir um abrangente sistema de supervisão pública sobre as atividades das plataformas digitais, impondo-lhes significativas obrigações substantivas e processuais.

Desse modo, o projeto de reforma do Código Civil incorporou diretrizes para a moderação de conteúdo, exigência de medidas para conter a propagação de conteúdo ilícito e obrigatoriedade de oferecer mecanismos eficazes para reclamações e reparações, além de reforçar os requisitos de transparência.

3.4 Patrimônio digital

O texto abaixo está contido no Capítulo V do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Do patrimônio digital".

CAPÍTULO V

PATRIMÔNIO DIGITAL

Art. 2.027-AA. Considera-se patrimônio digital o conjunto de ativos intangíveis e imateriais, com conteúdo de valor econômico, pessoal ou cultural, pertencente a pessoa ou entidade, existentes em formato digital.

Parágrafo único. A previsão deste artigo inclui, mas não se limita a dados financeiros, senhas, contas de mídia social, ativos de criptomoedas, *tokens* não fungíveis ou similares, milhagens aéreas, contas de games ou jogos cibernéticos, conteúdos digitais como fotos, vídeos, textos, ou quaisquer outros ativos digitais, armazenados em ambiente virtual.

Art. 2.027-AB. Os direitos de personalidade que se projetam

após a morte constantes de patrimônio essenciais e personalíssimos, tais como privacidade, intimidade, imagem, nome, honra, dados pessoais, entre outros, observarão o disposto em lei especial e no Capítulo II do Título I do Livro I da Parte Geral deste Código.

Art. 2.027-AC. A transmissão hereditária dos dados e informações contidas em qualquer aplicação de internet, bem como das senhas ou códigos de acesso, pode ser regulada em testamento.

§ 1º O compartilhamento de senhas ou de outras formas para acesso a contas pessoais será equiparado a disposições contratuais ou testamentárias expressas, para fins de acesso dos sucessores, desde que tais disposições estejam devidamente comprovadas.

§ 2º Integra a herança o patrimônio digital de natureza econômica, seja pura ou híbrida, conceituada a última como a que tenha relação com caracteres personalíssimos da pessoa natural ou jurídica.

§ 3º Os sucessores legais podem pleitear a exclusão da conta ou a sua conversão em memorial, diante da ausência de declaração de vontade do titular.

Art. 2.027-AD. Salvo expressa disposição de última vontade e preservado o sigilo das comunicações, e a intimidade de terceiros, as mensagens privadas do autor da herança difundidas ou armazenadas em ambiente virtual não podem ser acessadas por seus herdeiros, em qualquer das categorias de bens patrimoniais digitais.

§ 1º Mediante autorização judicial e comprovada a sua necessidade, o herdeiro poderá ter acesso às mensagens privadas da conta do falecido, para os fins exclusivos autorizados pela sentença e resguardados os direitos à intimidade e à privacidade de terceiros.

§ 2º O tempo de guarda das mensagens privadas do falecido pelas plataformas deve seguir legislação especial.

§ 3º Diante da ausência de declaração de vontade do titular, os sucessores ou representantes legais do falecido poderão pleitear a exclusão ou a manutenção da sua conta, bem como sua conversão em memorial, garantida a transparência de que a gestão da conta será realizada por terceiro.

§ 4º Serão excluídas as contas públicas de usuários brasileiros, quando, falecidos, não deixarem herdeiros ou representantes legais, contados 180 (cento e oitenta) dias da comprovação do óbito.

Art. 2.027-AE. São nulas de pleno direito, na forma do art. 166 deste Código, quaisquer cláusulas contratuais voltadas a restringir os poderes da pessoa, titular da conta, de dispor sobre os próprios dados e informações.

Art. 2.027-AF. O titular de um patrimônio digital tem o direito à proteção plena de seus ativos digitais, incluindo a proteção contra acesso, uso ou transferência não autorizados.

Art. 2.027-AG. Os prestadores de serviços digitais devem garantir medidas adequadas de segurança para proteger o patrimônio digital dos usuários e fornecer meios eficazes para que os titulares gerenciem e transfiram esses ativos, com plena segurança, de acordo com a sua vontade.

3.4.1 Abordagem teórica da temática

Como visto no item 3.3, o fenômeno da "plataformização da vida" tornou as plataformas digitais nos principais ambientes onde uma parcela substancial da população mundial conduz suas atividades econômicas, sociais, culturais e políticas, para trocar de informações, celebrar de contratos, dentre outras atividades, fazendo com que o legado digital assumisse um valor econômico e social relevante.

Nesse cenário, deve-se destacar que o uso do celular se tornou um elemento de grande impacto na constituição desse legado digital, já que reúne informações pessoais e íntimas. A crescente utilização do celular em todas as camadas da sociedade e por diferentes faixas etárias facilita a comunicação e a interação em todos os níveis, bem como o transforma num repositório de dados. A massificação de instrumentos que detém informações pessoais desafia questões relacionadas à privacidade.

O patrimônio, tradicionalmente, esteve associado a bens materiais. Porém, numa era de digitalização crescente, o conceito de patrimônio tem se expandido, abarcando tanto bens materiais como imateriais, que são constituídos nos ambientes físico e digital. Sobre esse ponto, a ministra Nancy Andrighi faz uma importante ressalva ao afirmar que: "Com o passar dos anos, o número de usuários mortos superará o de vivos, criando verdadeiros cemitérios virtuais" (2025, p. 118). Tal ponto é abordado pelo Projeto de Lei nº 4, de 2025 ao tratar da transmissão hereditária dos dados e das informações contidas em qualquer aplicação de internet.

Isso coloca em xeque categorias clássicas do direito civil patrimonial, de forma que a dicotomia entre bens materiais e bens imateriais, que estruturou as codificações modernas, revela-se insuficiente para tratar dos dilemas que envolvem os ativos digitais. Diante desse cenário, o patrimônio digital, pelas suas peculiaridades, vem se consolidando como uma subcategoria especial no âmbito dos bens imateriais, coexistindo com outros institutos, tais como os direitos de propriedade intelectual, os direitos da personalidade e os dados pessoais.

Conforme pontua Dierle Nunes (2025), as questões relativas à sucessão patrimonial se restringiam a verificar a existência de um testamento deixado pelo falecido e avaliar a validade dele, e, na ausência de tal documento, aplicar as normas estabelecidas pelo Código Civil e Código de Processo Civil para determinar a quem seriam destinados os bens. Porém, com a rápida evolução e disseminação de tecnologias, como a internet, *smartphones* e redes sociais, tornou-se evidente que o uso difundido desses é uma tendência irreversível e exige, portanto, a regulamentação específica dos ativos digitais.

O patrimônio digital representa, portanto, uma etapa recente no processo histórico de ampliação do conceito patrimonial, impulsionado pela transição para a sociedade da informação e pelo predomínio da economia de dados[21]. Esse novo cenário jurídico demanda, portanto, a revisão das regras de sucessão, a formulação de novos critérios para transmissibilidade dos ativos digitais a partir de um microssistema normativo próprio, nos moldes delineados pelo Projeto de Lei nº. 4, de 2025.

Como se verá mais adiante, o Projeto de Lei nº 4, de 2025, adotou a classificação trinária (Porto, 2024b), com as categorias essenciais e personalíssimas, patrimoniais e híbridas, de forma a prever as diversas possibilidades de constituição do patrimônio digital.

Os bens patrimoniais que se apresentam como aqueles cuja natureza é meramente econômica podem ser compreendidos como moedas virtuais, milhas aéreas, créditos e avatares em jogos virtuais, itens pagos em plataformas digitais, entre outros (Burille; Honorato; Leal, 2021). Tais exemplos são alguns dos bens digitais econômicos que refletem a realidade do mundo contemporâneo, devendo o direito acompanhar os novos paradigmas.

Com o crescente avanço da internet, monetização de contas e perfis em redes sociais, bem como o surgimento de novas profissões voltadas ao público on-line, surge a necessidade de uma terceira classificação para associar esses bens que tratam de direitos personalíssimos, ao mesmo tempo que possuem valor econômico. Como exemplo da rentabilidade de um bem de natureza híbrida, cita-se o perfil no Instagram do falecido

21 "Duas são as peculiaridades do conteúdo digital que acabam por impor desafios importantes na discussão sobre a transmissibilidade do conteúdo ou do acesso pelos herdeiros em caso de morte de seu titular: i) para além do conteúdo patrimonial dos bens digitais, eles exprimem, muitas vezes, um conteúdo extrapatrimonial, podendo afetar eventualmente direito de terceiro ou o direito de personalidade post mortem; ii) ao contrário de cartas, diários e livros armazenados na casa ou no ambiente de trabalho da pessoa falecida, o conteúdo digital é armazenado por um provedor de serviços de internet, que acaba determinando, por meio do contrato, um maior ou menor acesso do conteúdo aos herdeiros". (Mendes; Fritz, 2019, p. 192)

apresentador Gugu Liberato, que apresentou um elevado salto em número de seguidores após a divulgação de sua morte. Ocorre que essa conta era utilizada de forma pessoal pelo apresentador, motivo pelo qual seu acesso post mortem não foi automático. Nesse contexto, a própria plataforma do Instagram possibilita a exclusão da rede, após comprovado o óbito, ou a conversão em memorial. Nessa perspectiva, Leal (2019) expôs que determinados bens que possuem esse caráter dúplice – personalíssimo/patrimonial – são passíveis para integrar a herança. Uma das formas pacificadas de transmissão dos bens digitais, personalíssimos ou híbridos, é o próprio consentimento do usuário em vida, seja por testamento, seja por meio da transmissão dos dados.

A transmissibilidade do patrimônio digital, nos termos do Projeto de Lei nº 4, de 2025, será realizada a partir das seguintes premissas:

1) Deve respeitar a privacidade do falecido, considerando a intimidade tanto do próprio quanto de terceiros e interlocutores envolvidos. Portanto, o projeto de lei determina que, ao serem transmitidos, esses dados não deveriam permitir que os herdeiros acessem mensagens privadas, a não ser que caso haja autorização judicial.

2) Os ativos digitais com valor econômico, sejam eles de natureza pura ou híbrida, fazem parte da herança e devem ser repassados aos herdeiros, tai como criptomoedas, contas de investimento on-line, programas de milhagem e *tokens* não fungíveis (NFTs).

3) A transferência hereditária de dados e informações armazenados em qualquer aplicativo da internet, assim como das senhas ou códigos de acesso, pode ser regulamentada por meio de um testamento ou por meios administrativos disponibilizados pela própria plataforma.

Diante do exposto, verificamos que a importância do patrimônio digital está na sua capacidade de englobar bens de natureza patrimonial, de natureza existencial e bens híbridos. Nesse sentido, Laura Porto afirma que:

> A regulamentação proposta não só oferece segurança jurídica, mas também assegura que a memória digital dos indivíduos seja tratada com a devida consideração. Ao definir claramente como os bens digitais devem ser geridos após a morte, protegemos não apenas o valor econômico desses ativos, mas também a privacidade do falecido. As plataformas digitais, por sua vez, são incentivadas a criar mecanismos robustos que respeitem e facilitem a gestão desses bens conforme a vontade dos usuários. (Porto, 2024b)

Como bem ressalta a ministra Nancy Andrighi:

> Como consequência, a herança digital guarda a característica da patrimonialidade, típica do conceito tradicional de herança. Ou seja, esse setor do acervo hereditário é avaliável em pecúnia, embora, na hipótese concreta, não possua valor econômico. Além disso, a herança digital não é composta, em rigor, pelos

> bens digitais, mas pelas posições jurídicas patrimoniais que sobre eles recaem. Dessa forma, não integra a herança digital o perfil de determinado usuário no aplicativo Whatsapp, mas a posição jurídica titularizada em vida pelo de cujus fruto do contrato celebrado com a sociedade empresária que gerencia a plataforma. (Andrighi, 2025, p. 117)

Considerando que as plataformas digitais são repositórios importantes do patrimônio digital, deve-se verificar como as suas políticas internas estruturam suas diretrizes para acesso *post mortem* ao legado digital, como se verá a seguir.

3.4.2 O tratamento da matéria pelas plataformas digitais

a) Apple

No contexto do serviço de armazenamento em nuvem (iCloud), a Apple esclarece os termos do legado digital:

> Legado Digital. Com o Legado Digital, você pode escolher adicionar um ou mais contatos para terem acesso e baixar alguns dados de sua conta após a sua morte. Se os seus contatos designados fornecerem um certificado de óbito para a Apple e tiverem a chave necessária, eles terão acesso automaticamente a tais dados da conta e o bloqueio de ativação será removido de todos os seus dispositivos. Desta forma, é responsabilidade sua manter os contatos de Legado Digital atualizados. (Apple, 2025b)

Segundo as instruções da Apple, um Contato de Legado refere-se à pessoa designada por você para obter acesso aos dados da Conta Apple após o seu falecimento. É importante compreender quais informações serão compartilhadas com o Contato de Legado e conhecer o procedimento para adicionar um ou mais desses contatos:

> O Contato de Legado pode ser qualquer pessoa que você escolher. Além disso, você poderá designar mais de um Contato de Legado. A pessoa escolhida nem precisa ter uma Conta Apple ou um dispositivo Apple.
>
> Para fazer uma solicitação de acesso após o seu falecimento, é necessário apenas:
>
> A chave de acesso que você gerou quando escolheu o contato;
>
> Certidão de óbito.
>
> A Apple analisará solicitações de Contatos de Legado e dará acesso aos dados da sua Conta Apple somente depois de confirmar essas informações. Quando o acesso for aprovado, o Contato de Legado receberá uma Conta Apple especial, que poderá ser configurada e usada para acessar a conta. A Conta Apple não funcionará mais, e o Bloqueio de Ativação será removido em qualquer dispositivo que use sua Conta Apple. (Apple, 2025a)

b) Facebook

Há uma comunicação por parte do Facebook ao tomar conhecimento do falecimento de um usuário a fim de transformar a conta de um falecido em um memorial, exceto nos casos em que exista uma solicitação de exclusão por parte do próprio usuário antes de falecer ou de um membro da família, como se verifica abaixo.

> Quando o Facebook toma conhecimento de que uma pessoa faleceu, nossa política é transformar essa conta em memorial. As contas transformadas em memorial são um local em que amigos e familiares podem se reunir para compartilhar lembranças após o falecimento de uma pessoa. A transformação de uma conta em memorial também ajuda a protegê-la, impedindo que as pessoas entrem nela. (Facebook, 2025)

c) Google

A empresa disponibiliza aos usuários a opção de criar um "plano de gerenciamento de contas inativas". Ao acessar esse recurso, os usuários são informados de que o "Gerenciador de contas inativas" é o meio mais eficaz para indicar quem deverá ter acesso às informações quando a conta for considerada inativa. Além disso, possibilita que qualquer usuário apresente uma solicitação relacionada à conta de uma pessoa falecida, seja para requerer o encerramento dela ou, em determinadas circunstâncias, para obter acesso ao conteúdo. As informações referentes a esse procedimento são disponibilizadas aos usuários da plataforma:

> Enviar uma solicitação a respeito da conta de um usuário falecido
>
> As pessoas esperam que o Google mantenha suas informações seguras, mesmo no caso de falecimento.
>
> Fazer planos para sua conta
>
> O Gerenciador de contas inativas é a melhor maneira para você nos informar quem deve ter acesso às suas informações e se você deseja que sua conta seja excluída. Configure o Gerenciador de contas inativas para sua conta.
>
> Fazer uma solicitação para a conta de uma pessoa falecida
>
> Reconhecemos que muitas pessoas falecem sem deixar instruções claras sobre como gerenciar suas contas on-line. Podemos trabalhar com membros imediatos da família e com representantes para fechar a conta de uma pessoa falecida, quando apropriado. Em certas circunstâncias, podemos fornecer o conteúdo da conta de um usuário falecido. Em todos esses casos, nossa principal responsabilidade é manter as informações das pessoas seguras, protegidas e particulares. Não podemos fornecer senhas ou outros detalhes de login. Qualquer decisão de atender a uma solicitação sobre um usuário falecido será feita somente após uma cuidadosa análise. (Google, 2025)

d) Instagram

A plataforma proporciona aos usuários a opção de transformar a conta de uma pessoa falecida em um memorial ou de solicitar a exclusão dela, sendo esta última possibilidade disponível mediante a requisição de um familiar direto do falecido, como se verifica abaixo:

> Como denunciar a conta de uma pessoa falecida no Instagram
>
> Se você vir uma conta no Instagram que pertence a uma pessoa que faleceu, poderá solicitar a transformação da conta em memorial. Se você é um familiar direto dessa pessoa, pode solicitar que a conta seja removida do Instagram.
>
> Como transformar a conta em memorial
>
> Transformaremos em memorial a conta do Instagram de uma pessoa falecida quando recebermos uma solicitação válida. Tentamos evitar que as referências às contas transformadas em memorial apareçam no Instagram de forma que possa incomodar os amigos ou familiares da pessoa falecida. Além disso, tomamos medidas para garantir a privacidade dessa pessoa protegendo a conta dela.
>
> Para denunciar uma conta a ser transformada em memorial, fale conosco. Para transformar uma conta em memorial, precisamos de uma prova do falecimento, como o link para o obituário ou um artigo de jornal.
>
> Não podemos divulgar as informações de login de uma conta transformada em memorial. Entrar na conta de outra pessoa sempre viola nossas políticas.
>
> Como remover a conta
>
> Os familiares próximos confirmados podem solicitar a remoção da conta do Instagram de um ente querido. Quando você envia uma solicitação de remoção, solicitamos provas de que você é um familiar direto da pessoa falecida. Estes são alguns exemplos:
>
> A certidão de nascimento da pessoa falecida.
>
> A certidão de óbito da pessoa falecida.
>
> Comprovação de autoridade de acordo com a legislação local de que você é o representante legal da pessoa falecida ou de seu espólio.
>
> Para solicitar que uma conta seja removida, preencha este formulário (Instagram, 2025).

e) X (antigo Twitter)

A plataforma indica que, em caso de falecimento de um usuário, uma pessoa autorizada a agir em nome do Estado ou um parente próximo pode solicitar a desativação da conta. As condições para tal solicitação são descritas nos seguintes termos:

Como entrar em contato com o X para falar sobre a conta de um familiar falecido

Usuário falecido

Caso um usuário do X faleça, podemos trabalhar com uma pessoa autorizada a agir em nome do Estado ou com um parente imediato verificado do falecido para efetuar a desativação da conta.

Solicite a remoção da conta de um usuário falecido.

Solicite a remoção da conta de um usuário falecido. Depois de enviar sua solicitação, enviaremos a você um e-mail com instruções para fornecer mais detalhes, incluindo informações sobre a pessoa falecida, uma cópia de sua identidade e uma cópia da certidão de óbito da pessoa. Esta é uma etapa necessária para evitar denúncias falsas e/ou não autorizadas. Garantimos que essas informações permanecerão confidenciais e serão removidas assim que as tivermos examinado.

Nota: não podemos fornecer informações de acesso à conta a ninguém, independentemente do seu grau de relacionamento com o falecido. Veja mais informações sobre mídia no X relacionada a um familiar falecido (X, 2025).

3.4.3 Experiências normativas do direito estrangeiro

3.4.3.1 Alemanha

De acordo com o *Bundesgerichtshof* (Alemanha, 2018), as correspondências digitais são, em princípio, passíveis de serem transmitidas aos herdeiros, assim como as cartas e os diários pessoais. Isso ocorre porque, no ambiente digital, prevalece o princípio da sucessão universal, assim como no contexto material. Esse princípio, estabelecido no parágrafo 1922, inciso 1 do Código Civil Alemão (BGB), determina que todo o patrimônio de uma pessoa falecida, incluindo todas as relações jurídicas, é transmitido aos herdeiros, excetuando-se aquelas relações que se extinguem pela própria natureza, por imposição legal, acordo ou pela vontade manifesta do falecido. Nos casos não abrangidos por essas exceções, os herdeiros assumem imediatamente a titularidade das relações jurídicas do falecido com a abertura da sucessão, conforme o princípio da *saisine* (Fritz, 2019).

3.4.3.2 Espanha

A *Ley Orgánica* 3/2018, intitulada "*Protección de Datos Personales y garantía de los derechos digitales*", no artigo 96, determina que os herdeiros podem exercer os direitos de acesso, retificação ou exclusão dos dados pessoais do falecido, conforme se verifica abaixo:

Artigo 96.º. Direito a um testamento digital.

1. O acesso aos conteúdos geridos pelos prestadores de serviços da sociedade da informação relativos a pessoas falecidas rege-se pelas seguintes regras:

a) As pessoas com vínculo familiar ou de fato com o falecido, bem como os seus herdeiros, podem contactar os prestadores de serviços digitais para acessar esses conteúdos e fornecer-lhes as instruções que considerem adequadas quanto à sua utilização, destino ou eliminação.

Excepcionalmente, as referidas pessoas não podem acessar os conteúdos do falecido, nem solicitar a sua modificação ou eliminação, quando o falecido o tiver expressamente proibido ou quando a lei assim o estabelecer. Esta proibição não afeta o direito dos herdeiros de acessar os conteúdos que possam fazer parte do espólio do falecido.

b) O testamenteiro, bem como qualquer pessoa ou instituição expressamente designada pelo falecido para esse fim, também poderá solicitar, de acordo com as instruções recebidas, o acesso ao seu conteúdo, a fim de cumprir as mesmas.

c) No caso de menores falecidos, estes poderes poderão também ser exercidos pelos seus representantes legais ou, no âmbito das suas competências, pelo Ministério Público, que poderá atuar de ofício ou a requerimento de qualquer pessoa física ou jurídica interessada.

d) No caso de falecimento de pessoas com deficiência, estes poderes poderão também ser exercidos, para além dos indicados na alínea anterior, por aqueles designados para o exercício de funções de apoio, desde que tais poderes se entendam incluídos nas medidas de apoio prestadas pela pessoa designada.

2. As pessoas autorizadas no número anterior poderão decidir pela manutenção ou eliminação dos perfis pessoais de pessoas falecidas nas redes sociais ou serviços equivalentes, salvo se o falecido tiver decidido sobre esta circunstância, caso em que se aplicarão as suas instruções.

O responsável pelo serviço a quem for comunicada a solicitação de eliminação do perfil, nos termos do parágrafo anterior, deverá proceder à mesma sem demora.

3. Os requisitos e condições para a comprovação da validade e eficácia dos mandatos e instruções, e, se for o caso, do seu registo, serão estabelecidos por decreto real. Este poderá coincidir com o disposto no artigo 3.º desta Lei Orgânica. (Espanha, 2018).(Tradução nossa)[22]

22 No original: "Artículo 96. Derecho al testamento digital.

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán

3.4.3.3 Síntese analítica das experiências normativas do direito estrangeiro

As experiências normativas estrangeiras revelam que a regulamentação sucessória do patrimônio digital é uma tendência mundial, com certa semelhança de tratamento da matéria. Em alguns países, como a Alemanha, há a transmissão automática dos ativos digitais aos herdeiros, salvo disposição em contrário do falecido e em algumas hipóteses legais previstas. Em sentido semelhante a Espanha regulamentou a matéria. Assim, o Projeto de Lei nº 4, de 2025, representa um avanço ao preencher essa lacuna no ordenamento jurídico brasileiro, incorporando soluções que já vêm sendo implementadas em outros países.

3.4.4 Estudos de caso

3.4.4.1 Alemanha

O *leading case* sobre herança digital, ocorrido na Alemanha, foi o primeiro em que o *Bundesgerichtshof* reconheceu a possibilidade de transmissão da herança digital para os herdeiros dos usuários de redes sociais (Alemanha, 2018). No caso paradigmático, a Corte alemã determinou que, em conformidade com os princípios de autonomia privada e autodeterminação, cabe ao titular decidir o destino da própria herança digital, podendo escolher impedir a transmissão dela ou nomear um responsável para acessar e gerenciar o conteúdo digital. Na ausência de uma determinação explícita por parte do titular falecido, aplica-se a regra geral estabelecida no ordenamento jurídico, que autoriza os herdeiros a tomarem essa decisão.

---

dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica." (Espanha, 2018).

Em 2012, após o trágico falecimento da filha de 15 anos em um acidente no metrô de Berlim, os pais de uma adolescente moveram uma ação judicial contra o Facebook alegando que a plataforma os impediu de acessar a conta da filha, a qual havia sido convertida em um perfil de "memorial". As circunstâncias que envolveram a morte da jovem permaneciam incertas, e os pais da jovem objetivavam acessar a conta para compreender as causas que sugeriam a possibilidade de suicídio e ocorrência de assédio escolar.

Após a transformação da conta em memorial, as informações que a falecida havia compartilhado publicamente continuavam acessíveis, permitindo que indivíduos pudessem postar mensagens no perfil da menina. No entanto, o acesso ao conteúdo de comunicação privada, incluindo conversas e fotos armazenadas na conta, permanecia restrito e inacessível a qualquer pessoa.

Em 17 de dezembro de 2015, o juiz de primeira instância (LG Berlin, 2015) decidiu em favor dos pais da adolescente, determinando que o Facebook concedesse acesso à conta da filha falecida. O magistrado fundamentou a decisão no entendimento de que a herança digital da falecida pertencia legitimamente aos herdeiros, permitindo-lhes, assim, acesso a todas as contas de e-mail, dispositivos móveis, aplicativos como WhatsApp e outras plataformas de redes sociais associadas.

Em instância recursal, o *Kammergericht* revisou a decisão anterior, reconhecendo, em teoria, os direitos e as obrigações decorrentes de contratos, como do Facebook, que podem ser transferidos através da herança, o tribunal destacou a falta de clareza jurídica quanto à transmissibilidade de bens de natureza estritamente pessoal e proibiu o acesso à conta com base no argumento de que tal ação violaria o sigilo das comunicações dos interlocutores da falecida.

A família apelou ao *Bundesgerichtshof* (Alemanha, 2018), que, em 12 de julho de 2018, reconheceu o direito dos pais como herdeiros legais para acessar a conta da filha falecida, bem como todo o conteúdo armazenado nela. O tribunal federal alemão argumentou que esse direito emergia do contrato de consumo entre a adolescente e o Facebook, que, com o falecimento, poderia ser transmitido aos herdeiros.

3.4.4.2 Brasil: Tribunal de Justiça de Minas Gerais

Em sede de Agravo de Instrumento, o Tribunal de Minas Gerais (TJMG) não permitiu o acesso à conta Apple do *de cujus*. O agravante alega que a "nuvem" da conta Apple do falecido detinha um grande acervo de fotografias de grande valor sentimental para a família, mas o tribunal entendeu que esse acesso violaria o direito à personalidade e à imagem do falecido, conforme se verifica abaixo:

> EMENTA: AGRAVO DE INSTRUMENTO. INVENTÁRIO. HERANÇA DIGITAL. BENS DIGITAIS EXISTENCIAIS. DESBLOQUEIO DE ACESSO APPLE PERTECENTE AO DE CUJUS. PEDIDO DE ACESSO ÀS INFORMAÇÕES PESSOAIS DO FALECIDO.

ACERVO FOTOGRÁFICO E CORRESPONDÊNCIAS GUARDADOS EM NUVEM. INDEFERIMENTO. VIOLAÇÃO A DIREITO DA PERSONALIDADE E DA IMAGEM DO FALECIDO. PROTEÇÃO À INTIMIDADE E A VIDA PRIVADA DO DE CUJUS. AUTONOMIA EXISTENCIAL. NECESSIDADE DE GARANTIA. RECURSO NÃO PROVIDO.

– A Constituição Federal consagrou, em seu artigo 5º, a proteção constitucional ao direito à intimidade (são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação).

– A herança defere-se como um todo unitário, o que inclui não só o patrimônio material do falecido, como também o imaterial, em que estão inseridos os bens digitais de vultosa valoração econômica, denominada pela doutrina de "herança digital", desde que tenham valor econômico.

– Os bens digitais patrimoniais poderiam ser, assim, objeto de sucessão, devendo ser arrolados no inventário, para que se opere a transmissão causa mortis, enquanto em relação aos bens digitais existenciais (fotos, arquivos, vídeos e outros guardados em nuvem com senha), não seria possível dispensar tal tratamento, por se tratarem de questões vinculadas aos direitos da personalidade, intransmissíveis e de caráter eminentemente pessoal do falecido.

– Eventual transmissão sucessória de acervos digitais particulares poderá acarretar violação dos direitos da personalidade, que são, via de regra, intransmissíveis e se perpetuam, mesmo após a morte do sujeito.

– A autorização judicial para o acesso às informações privadas do usuário falecido deve ser concedida apenas nas hipóteses em que houver relevância econômica, a justificar o acesso aos dados mantidos como sigilosos, pelo próprio interessado, através de senha ou biometria, sem qual quer menção a possibilidade de sucessão ou de compartilhamento.

– Os dados pessoais do de cujus são merecedores de proteção jurídica no âmbito da Internet.

– Se o falecido quisesse que outras pessoas tivessem acesso a seu acervo fotográfico, disponível apenas em "nuvem" digital, teria compartilhado, impresso, feito backup ou realizado o salvamento em algum lugar de livre acesso por terceiros (sem senha), repassado ou anotado a mesma em algum lugar.

– Deve-se considerar a vontade manifestada pelo usuário em vida a respeito do destino dos conteúdos inseridos por ele na rede, no que for compatível com o ordenamento jurídico interno e com os termos de uso dos provedores, como forma de consagração de sua autonomia existencial. Na ausência de disposição de vontade, devem ser aplicadas as previsões contidas nos termos de uso dos provedores.

– Recurso conhecido, mas não provido (Tribunal de Justiça do Estado de Minas Gerais, 2024).

Neste outro caso, o Agravo de Instrumento 1.0000.21.190675-5/001, o Tribunal de Justiça de Minas não autorizou o desbloqueio de dispositivos eletrônicos do falecido, justamente com o fim de proteger os direitos dele *post mortem*. Nesse caso, a agravante almejava o desbloqueio de um celular e um notebook devido aos seus valores econômicos.

> EMENTA: AGRAVO DE INSTRUMENTO. INVENTÁRIO. HERANÇA DIGITAL. DESBLOQUEIO DE APARELHO PERTECENTE AO DE CUJUS. ACESSO ÀS INFORMAÇÕES PESSOAIS. DIREITO DA PERSONALIDADE. A herança defere-se como um todo unitário, o que inclui não só o patrimônio material do falecido, como também o imaterial, em que estão inseridos os bens digitais de vultosa valoração econômica, denominada herança digital. A autorização judicial para o acesso às informações privadas do usuário falecido deve ser concedida apenas nas hipóteses que houver relevância para o acesso de dados mantidos como sigilosos. Os direitos da personalidade são inerentes à pessoa humana, necessitando de proteção legal, porquanto intransmissíveis. A Constituição Federal consagrou, em seu artigo 5o, a proteção constitucional ao direito à intimidade. Recurso conhecido, mas não provido (Tribunal de Justiça do Estado de Minas Gerais, 2022).

3.4.4.3 Brasil: Tribunal de Justiça da Paraíba

Em contrapartida, há casos em que essa privacidade é relativizada por alguns motivos, como a anterior disponibilização das senhas e dados ao herdeiro, ou então alteração das redes sociais para *in memoriam*, como é o caso do Agravo Interno abaixo:

> AGRAVO INTERNO. DECISÃO QUE PROIBIU EXCLUSÃO DE CONTAS EM FACEBOOK E INSTAGRAM DE PESSOA FALECIDA. POSSIBILITANDO ACESSO DO EX-CÔNJUGE AO PERFIL COMO MEMORIAL. DADOS DE FOTOS DO AGRAVANTE E CASAL QUE INTERESSAM À FAMÍLIA. DIREITO HEREDITÁRIO PRESERVAÇÃO DA INTIMIDADE DA FALECIDA COM EXCLUSÃO DE CONVERSAS PARTICULARES ANTERIORES AO SEU ÓBITO. DECISÃO QUE NÃO CAUSA PREJUÍZO À EMPRESA. MANUTENÇÃO. DESPROVIMENTO DO AGRAVO INTERNO (Tribunal de Justiça do Estado da Paraíba, 2023).

3.4.4.4 Brasil: Tribunal de Justiça de São Paulo

Outro exemplo de exceção foi a Apelação nº 1123920-82.2023.8.26.0100, na qual o Tribunal de Justiça de São Paulo possibilitou à genitora acessar algumas contas de seu falecido filho com o fim de obter informações a respeito de sua morte, tendo em vista uma das hipóteses de sua causa: suicídio.

> APELAÇÃO. Direito digital. Pedido de fornecimento de acesso às contas de e-mail e aplicativo de mensagens que seriam do filho falecido da autora. Sentença de improcedência. Ausência de comprovação da titularidade das contas. Recurso da autora. Dados acerca da titularidade da conta de e-mail que é armazenado pelo próprio provedor. Impossibilidade de exigir da apelante, no caso concreto, que produza prova categórica desse fato. "Herança digital" que não encontra regulamentação no Brasil. Possibilidade de analogia com a herança de cartas e manuscritos pessoais. Comparação com interceptação telefônica que não prospera. Possibilidade de a sucessora herdar esse acervo de informações. Legítimo interesse em elucidar a morte precoce e não explicada do filho da apelante. Circunstâncias do caso concreto que devem prevalecer. Procedência com relação ao Google, para determinar o fornecimento de dados de acesso a contas que pertençam ao falecido. Impossibilidade técnica de fornecimento de registros de comunicações via WhatsApp. Mensagens que notoriamente são criptografadas de ponta a ponta. RECURSO PARCIALMENTE PROVIDO (Tribunal de Justiça do Estado de São Paulo, 2024).

Em contrapartida, há também julgados que relativizam o direito à privacidade mediante sólida argumentação e conformidade com a lei, como foi no processo de nº 1036531-51.2018.8.26.0224. Neste caso, o Tribunal de Justiça de São Paulo concedeu acesso aos e-mails do *de cujus* durante o período em que ele realizou tratativas com uma imobiliária, pois a requerente alegava que esses documentos viriam a instruir o inventário e confirmar que houve a contratação de seguro de vida.

3.4.5 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.4.5.1 Projeto de Lei nº 5.820/2019

O Projeto de Lei nº5820/2019, de iniciativa do deputado Elias Vaz, estabelece a alteração dos arts. 1.862, 1.864, 1.876 e 1.881 do Código Civil e dispõe sobre o testamento e codicilo digitais.

3.4.5.2 Projeto de Lei nº 6.468/2019

O Projeto de Lei nº6.468/2019, de iniciativa do senador Jorginho Mello, altera o art. 1788 do Código Civil, incluindo o parágrafo único para prever que serão transmitidos aos herdeiros todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança.

3.4.5.3 Projeto de Lei nº 3.050/2020

O Projeto de Lei nº3050/2020, de iniciativa do deputado Gilberto Abramo, propõe a alteração do art. 1.788 do Código Civil, a fim de dispor sobre a sucessão dos bens e as contas digitais do autor da herança de qualidade patrimonial.

3.4.5.4 Projeto de Lei nº 410/2021

O Projeto de Lei nº410/2021, de iniciativa do deputado Carlos Bezerra, acrescenta um artigo à Lei do Marco Civil da Internet para regular a situação das contas de internet após a morte do titular.

3.4.5.5 Projeto de Lei nº 1.144/2021

O Projeto de Lei nº1.144/2021, de iniciativa da deputada Renata Abreu está apensado ao Projeto de Lei 3050/2020. O referido projeto dispõe sobre os dados pessoais inseridos na internet após a morte do usuário.

3.4.5.6 Projeto de Lei nº 2.664/2021

O Projeto de Lei nº2.664/2021, apensado do Projeto de Lei nº 3.050/2020, de iniciativa do deputado Carlos Henrique Gaguim, propõe adicionar o artigo 1857-A ao Código Civil, para regulamentas a herança digital.

3.4.5.7 Projeto de Lei nº 365/2022

O Projeto de Lei nº365/2022, de iniciativa do senador Confúcio Moura, trata da herança digital que se relaciona com os direitos da personalidade e não possuam conteúdo patrimonial. As disposições relativas à herança digital podem ser especificadas em um testamento ou, quando essa funcionalidade estiver disponível, diretamente nas plataformas de internet.

3.4.5.8 Projeto de Lei nº 703/2022

O Projeto de Lei nº 703/2022, de iniciativa do deputado Hélio Lopes, acrescenta o art. 1857-A ao Código Civil, dispondo sobre a herança digital e possibilidade da pessoa dispor, por qualquer meio no qual fique expressa a manifestação de vontade, sobre o tratamento de dados pessoais após a sua morte.

3.4.6 Comentários sobre o texto do projeto da reforma do Código Civil

Analisando a legislação brasileira, verifica-se que a herança digital não é expressamente regulamentada pelos principais diplomas legais do regime do direito digital, como a Lei nº 12.965/2014 (Marco Civil da Internet), ou a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). No âmbito sucessório, o Código Civil em vigor, no art. 1.784, preceitua que, uma vez aberta a sucessão com a morte da pessoa natural, a herança transmite-se, desde logo, aos herdeiros e testamentários. Com base no princípio da *saisine*, implicitamente contido no caput do art. 1.784 do CC, o falecido, no momento da morte, transmite aos seus sucessores a posse e propriedade da herança, desde que

o herdeiro esteja vivo ou concebido no momento da herança, bem como não seja incapaz de herdar. Nesse sentido, o Projeto de Lei nº 4, de 2025, preenche uma lacuna importante ao trazer o conceito de patrimônio digital[23].

O projeto de lei conceitua patrimônio digital como um "conjunto de ativos intangíveis e imateriais, com conteúdo de valor econômico, pessoal ou cultural, pertencente a pessoa ou entidade, existentes em formato digital", destacando que esse conceito abrange, mas não se limita a dados financeiros, senhas, contas de mídia social, ativos de criptomoedas, tokens não fungíveis ou similares, milhagens aéreas, contas de games ou jogos cibernéticos, conteúdos digitais como fotos, vídeos, textos ou quaisquer outros ativos digitais, armazenados em ambiente virtual.

Além disso, prevê que o titular de um patrimônio digital possui o direito à integral proteção dos próprios ativos digitais, o que abrange a salvaguarda contra acessos, utilizações ou transferências não autorizadas. Já os prestadores de serviços digitais têm a responsabilidade de assegurar medidas de segurança apropriadas para proteger o patrimônio digital dos usuários. Além disso, devem oferecer mecanismos eficazes que permitam aos titulares gerenciar e transferir esses ativos de maneira segura e conforme a própria vontade, em clara consagração do direito à autodeterminação informativa do usuário.

Sobre a transmissão hereditária dos dados e das informações contidas em qualquer aplicação de internet, incluindo senhas ou códigos de acesso, o projeto de lei indica que essa pode ser regulada em testamento, "corroborando a evidente pós-eficácia dos direitos de personalidade" (Nunes, 2025, p. 417). Segundo Laura Porto, "a subcomissão de direito digital colocou o respeito à privacidade do falecido como premissa, respeitando tanto sua intimidade como dos possíveis terceiros e interlocutores envolvidos". (2024b)

Como já ressaltado, o projeto de lei adotou a classificação trinária (2024b), com as categorias essenciais e personalíssimas, patrimoniais e híbridas:

a) As informações e os dados de natureza essencial e personalíssima incluem aqueles que detêm apenas valor pessoal, como é o caso das mensagens privadas.

b) Os bens patrimoniais compreendem ativos com valor econômico associado, como criptomoedas, contas de investimentos digitais, milhas aéreas e outros bens digitais que podem ser mensurados financeiramente.

c) Os bens híbridos apresentam características de ambas as naturezas e não apenas detêm um valor pessoal relevante, mas também possuem um valor econômico associado. Um exemplo típico desse tipo de ativo seria uma conta de mídia social que gera receita.

23 "Art 2.027-AA. Considera-se patrimônio digital o conjunto de ativos intangíveis e imateriais, com conteúdo de valor econômico, pessoal ou cultural, pertencente a pessoa ou entidade, existentes em formato digital. Parágrafo único. A previsão deste artigo inclui, mas não se limita a dados financeiros, senhas, contas de mídia social, ativos de criptomoedas, tokens não fungíveis ou similares, milhagens aéreas, contas de games ou jogos cibernéticos, conteúdos digitais como fotos, vídeos, textos, ou quaisquer outros ativos digitais, armazenados em ambiente virtual".

O projeto de lei prevê, ainda, que os sucessores legais podem pleitear a exclusão da conta ou a conversão dela em memorial, diante da ausência de declaração de vontade do titular. As plataformas digitais deverão excluir as contas públicas de usuários brasileiros, quando, falecidos, não deixarem herdeiros ou representantes legais, contados 180 dias da comprovação do óbito, afastando a possibilidade das big techs serem herdeiras universais dos bens digitais de uma pessoa falecida.

Sobre o acesso às mensagens privadas do autor da herança, difundidas ou armazenadas em ambiente virtual, o projeto de lei indica que, salvo por expressa disposição de última vontade e preservado o sigilo das comunicações, tais mensagens não podem ser acessadas pelos herdeiros, em qualquer das categorias de bens patrimoniais digitais, de forma a preservar a intimidade do falecido.

Contudo, mediante a autorização judicial e comprovada necessidade, o herdeiro poderá ter acesso às mensagens privadas da conta do falecido para os fins exclusivos autorizados pela sentença e resguardados os direitos à intimidade e à privacidade de terceiros, o que refuta a equivocada ideia de intransmissibilidade irrestrita (Nunes, 2025).

Sobre o prazo de armazenamento das mensagens privadas do falecido, o projeto de lei remete à regulamentação pela legislação especial.

As cláusulas contratuais das plataformas digitais e dos sites que restrinjam os poderes da pessoa, titular da conta, de dispor sobre os próprios dados e informações são nulas de pleno direito.

Dessa forma, Porto (2024b) conclui que:

a) A regulamentação proposta proporciona não apenas segurança jurídica, mas também garante que a memória digital dos indivíduos seja tratada com a devida consideração;

b) Ao estabelecer, de maneira clara, as diretrizes para o gerenciamento dos bens digitais após o falecimento, protege-se tanto o valor econômico desses ativos quanto a privacidade do falecido;

c) Além disso, as plataformas digitais são instigadas a desenvolver mecanismos eficazes que respeitem e facilitem a administração desses bens de acordo com os desejos expressos pelos usuários;

d) Estabelece uma estrutura nítida e equitativa para a administração de bens digitais, assegurando que os desejos do titular sejam devidamente respeitados e os herdeiros possam acessar e gerir esses ativos de maneira segura e eficiente.

3.5 A presença e a identidade de crianças e adolescentes no ambiente digital

O texto abaixo está contido no Capítulo VI do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "A presença e a identidade de crianças e adolescentes no ambiente digital".

CAPÍTULO VI

A PRESENÇA E A IDENTIDADE DE CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL

Art 2.027-AH. É garantida a proteção integral de crianças e adolescentes no ambiente digital, observado o seu melhor e superior interesse, nos termos do estatuto que os protege e deste Código, estabelecendo-se, no ambiente digital, um espaço seguro e saudável para sua utilização.

Art. 2.027-AI. É dever de todos os provedores de serviços digitais:

I - implementar sistemas eficazes de verificação da idade do usuário para garantir que conteúdos inapropriados não sejam acessados por crianças e adolescentes;

II - proporcionar meios para que pais e responsáveis tenham condições efetivas de limitar e monitorar o acesso de crianças e adolescentes a determinados conteúdos e funcionalidades dispostos no ambiente digital;

III - assegurar a proteção de dados pessoais de crianças e adolescentes, na forma da Lei nº 13.709, de 14 de agosto de 2018.

IV - proteger os direitos das crianças e adolescentes desde o *design* do ambiente digital, garantindo que, em todas as etapas relativas ao desenvolvimento, fornecimento, regulação, gestão de comunidades, comunicação e divulgação de seus produtos e serviços, o melhor e superior interesse da criança e do adolescente sejam observados.

Art. 2.027-AJ. Os produtos ou serviços de tecnologia da informação destinados a crianças e a adolescentes serão concebidos, projetados, desenvolvidos, ofertados, comercializados, disseminados, compartilhados, transmitidos e operados considerando a garantia de sua proteção integral e a prevalência de seus interesses.

Parágrafo único. Os criadores dos produtos ou serviços previstos no *caput* deste artigo devem:

I – considerar os direitos, a capacidade e os limites das crianças e adolescentes a que se destinem, desde a sua concepção e projeto, e durante sua execução, disponibilização e utilização, devendo, por padrão, adotar opções que maximizem a proteção de sua privacidade e reduzam a coleta e utilização de dados pessoais;

II – utilizar linguagem clara e concisa, compreensível e adequada, compatível com a idade das crianças e dos adolescentes a que se destinem;

III – garantir a privacidade e a segurança das crianças e dos adolescentes, conforme seu estatuto e este Código, bem como demais direitos assegurados na Constituição Federal, em Tratados e Convenções em que o Brasil seja signatário, tais como a Convenção dos Direitos da Criança das Nações Unidas.

Art. 2.027-AK. É vedada a veiculação de publicidade nos produtos ou serviços de tecnologia da informação destinados a crianças e a adolescentes.

Parágrafo único. Aplica-se o disposto no *caput* deste artigo a toda forma de exibição de produtos ou de serviços, ainda que gratuitos, destinados a crianças ou a adolescentes, inclusive por meio de plataformas de compartilhamento de vídeo, de redes sociais e de outros produtos ou serviços de tecnologia da informação.

3.5.1 Abordagem teórica da temática

O uso de dispositivos eletrônicos e a presença de crianças e adolescentes no ambiente digital apresentam benefícios e riscos, principalmente quando o uso é excessivo ou inadequado. O tempo excessivo diante das telas pode resultar em atrasos no desenvolvimento, problemas de saúde, dificuldades na aprendizagem e mesmo questões emocionais e sociais[24].

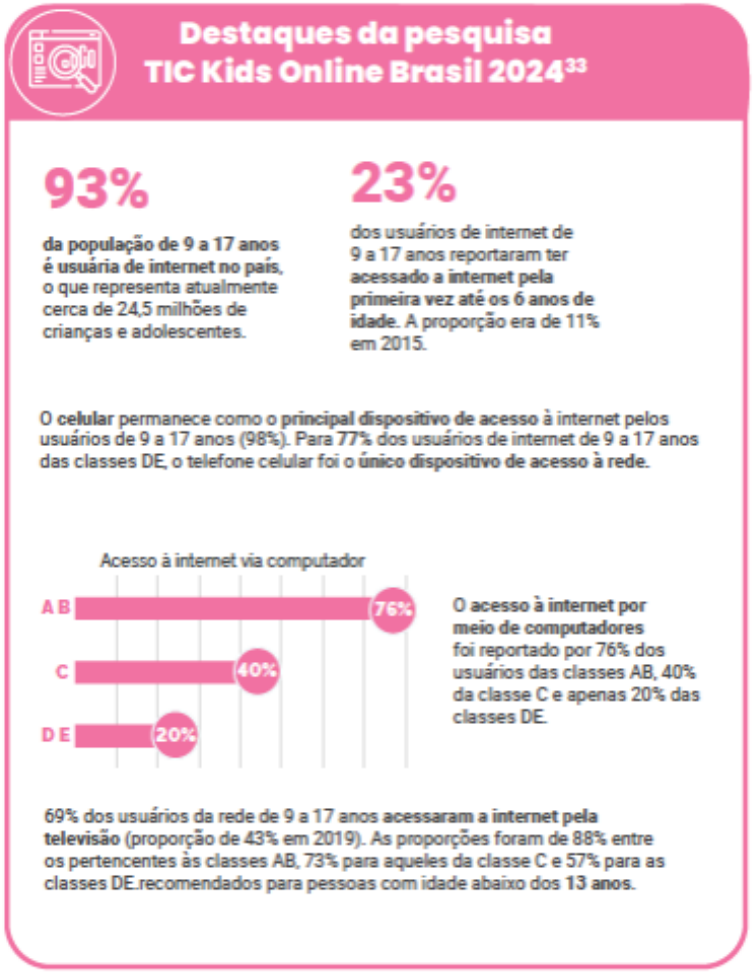
No Brasil, a Sociedade Brasileira de Pediatria (2024) recomenda que: a) crianças menores de 2 anos evitem o contato com telas; b) Para crianças entre 2 e 5 anos, o uso de telas deve ser limitado a uma hora diária, preferencialmente na companhia de um adulto; c) Para crianças de 6 a 10 anos, é indicado que o tempo de tela seja estendido

24 Importante estudo foi realizado pelo Instituto Veredas sobre os riscos do tempo excessivo diante das telas. Cf. BEIDACKI, C.; FARIAS, B.; BENATTI, G.; BOEIRA, L. Tempo de tela para crianças e adolescentes: respostas rápidas para governos – evidências, desafios e caminhos possíveis. São Paulo: Instituto Veredas, 2024. Disponível em: https://www.veredas.org/wordpveredas/wp-content/uploads/2024/07/OK-VOL-2_Veredas_Respostas-Rapidas_Final2-1.pdf. Acesso em: 20 maio 2025.

para até duas horas por dia; d) Para a faixa etária entre 11 e 17 anos, até três horas de exposição.

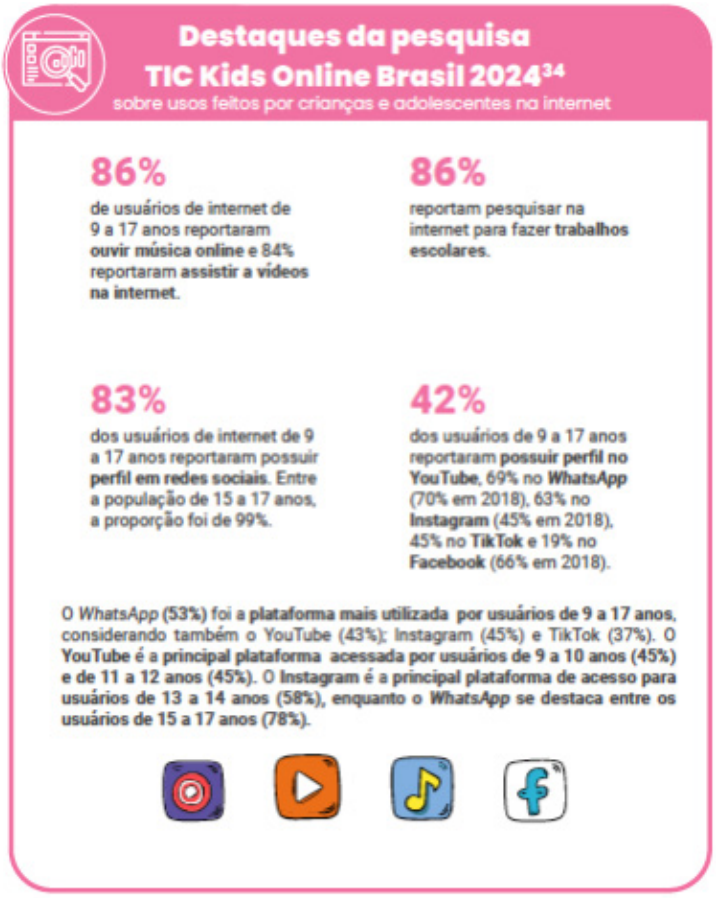
A Secretaria de Comunicação publicou o "Guia de Uso Consciente de Telas e Dispositivos Digitais para Crianças e Adolescentes" (Brasil, 2024), com dados e importantes recomendações para fomentar uma interação mais equilibrada entre os crianças e adolescentes brasileiros e o mundo digital. O referido guia analisou e consolidou dados do Comitê Gestor da Internet no Brasil sobre atuação de crianças e adolescentes no ambiente digital em 2024:

Figura 12 – Dados sobre o acesso à internet e ao celular pela população entre 9 e 17 anos



Fonte: Comitê Gestor da Internet no Brasil (2024). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024. São Paulo: CGI.br. Disponível em: https://cetic.br/pt/pesquisa/kids-online/indicadores/

Figura 13 – Dados sobre o uso da internet e de celular pela população entre 9 e 17 anos



Fonte: Comitê Gestor da Internet no Brasil (2024). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024. São Paulo: CGI.br. Disponível em: https://cetic.br/pt/pesquisa/kids-online/indicadores/

O guia traz um conceito interessante sobre cidadania digital:

> [...]uma vez que crianças e adolescentes circulam pelo ambiente digital, é fundamental compreender que a sua proteção está vinculada à regulação das plataformas (regras), à educação e empoderamento dos sujeitos adultos e infantojuvenis (pessoas) para lidar com as demandas desse contexto e ao desenvolvimento de experiências seguras e potentes (processos), como eixos estruturantes dos produtos/serviços disponíveis.[...]
>
> A cidadania digital envolve:
>
> • A condição de ser cidadão ou cidadã nos ambientes digitais de interação (como as redes sociais), assim como nos ambientes não virtuais, que podem ser impactados diretamente pelo uso de tecnologias digitais;
>
> • O conjunto de direitos e deveres criados para regular a interação entre as

pessoas durante o uso de tecnologias digitais, inclusive com a criação de leis específicas contra crimes cometidos nos ambientes virtuais de interação;

• O próprio exercício do conjunto de direitos civis, políticos e sociais na atualidade, exercício esse que pode ser facilitado ou não pelo acesso e uso responsável, ético e seguro das tecnologias digitais. (Brasil, 2024)

Para o exercício pleno e saudável desta cidadania, o guia traz importantes recomendações:

1.Crianças e adolescentes vivem intensas mudanças do crescimento e desenvolvimento corporal, mental e psicossocial, influenciadas por fatores externos, ambientais e culturais. O conjunto de evidências científicas disponíveis atualmente aponta que usos problemáticos ou excessivos de dispositivos digitais por crianças e adolescentes estão associados a diversos atrasos no desenvolvimento cognitivo, emocional e da linguagem, bem como a problemas de saúde e sofrimento mental.

2. Um dos fatores que mais contribuem para o uso precoce e excessivo de dispositivos digitais por crianças e adolescentes é o uso excessivo por parte dos adultos, que são modelos e referências de comportamento.

3. Decisões sobre o uso de dispositivos digitais nos ambientes familiares ou escolares devem sempre levar em conta os direitos à proteção integral, melhor interesse, a autonomia progressiva e a participação de crianças e adolescentes.

4. Empresas que desenvolvem aplicativos que possam ser usados por crianças e adolescentes devem investir em estratégias de verificação da idade, oferecer produtos ou serviços com base em princípios de segurança por design, coletar o mínimo necessário de dados, não expor crianças à comunicação mercadológica (inclusive de apostas), combater o trabalho infantil e ampliar a disponibilidade e divulgação de ferramentas que auxiliem processos de mediação familiar.

5. Todos aqueles para os quais a legislação brasileira prevê responsabilidade compartilhada sobre crianças e adolescentes devem colaborar para a garantia do direito à privacidade (interpessoal, institucional e comercial) de tais sujeitos, na relação com o ambiente digital.

6. Políticas de Educação Digital e Midiática ajudam a desenvolver habilidades para o uso adequado e a aproveitar os benefícios de dispositivos digitais e aplicativos, além de auxiliarem na redução dos riscos para crianças e adolescentes no ambiente digital.

7. A implementação de normas gerais sobre regulação do uso de celulares em unidades escolares deve orientar-se pela Lei Federal n° 15.100/2025, considerando a importância da autonomia pedagógica, da gestão democrática e da participação da comunidade escolar.

8. O uso de dispositivos digitais deve se dar aos poucos, conforme vá aumentando a autonomia progressiva da criança ou adolescente:

- Recomenda-se o não uso de telas e aparelhos digitais para crianças com menos de 2 anos, salvo para contato com familiares por videochamada, acompanhada de pessoa adulta;
- Orienta-se que crianças (antes dos 12 anos) não devem possuir aparelhos celulares do tipo smartphone próprios, sendo que, quanto mais tarde se der a posse ou aquisição de aparelho próprio, melhor;
- Acesso a redes sociais deve observar a faixa etária sinalizada pela Classificação Indicativa, através de ícones quadrados coloridos vinculados aos aplicativos nas lojas virtuais onde podem ser baixados. Reforça-se que a maioria das redes sociais não foi projetada para crianças, contendo padrões que estimulam o uso prolongado e potencialmente problemático, além de que a presença de crianças nelas pode pressionar outras a fazerem o mesmo, pelo receio de se sentirem excluídas daquele ambiente;
- O uso de dispositivos eletrônicos, aplicativos e redes sociais durante a adolescência (12 a 17 anos) deve se dar com acompanhamento familiar ou de educadores;
- O uso não pedagógico de dispositivos digitais no ambiente escolar, em qualquer etapa de ensino, pode trazer prejuízos para o processo de aprendizagem e desenvolvimento de crianças e adolescentes;
- Escolas devem avaliar criteriosamente o uso de aparelhos, como celulares ou tablets, para fins pedagógicos na Primeira Infância, evitando seu uso individual pelos estudantes aparelhos celulares próprios, bem como o uso de aplicativos de mensagem, por crianças (antes dos 12 anos).
- Deve ser estimulado o uso de dispositivos digitais, para fins de acessibilidade ou superação de barreiras, por crianças ou adolescentes com deficiência, independentemente de faixa etária. (Brasil, 2024)

A tutela da criança e do adolescente no contexto digital demanda o alargamento das tradicionais garantias fundamentais, de modo a contemplar as novas vulnerabilidades decorrentes das exposições tecnológicas e informacionais próprias desse ambiente. De acordo com o Estatuto da Criança e do Adolescente (ECA), o objetivo da proteção integral é facultar o desenvolvimento físico, mental, moral espiritual e social em condições de liberdade e dignidade, seja por lei ou por qualquer outro meio (art. 3º do ECA). Esses objetos de proteção e promoção são viscerais quando se trata dos limites e das consequências da vida digital das crianças e dos adolescentes. Essa previsão legal, que vige no direito brasileiro desde a década de 1990, já seria suficiente para, mesmo que de forma generalizada, limitar e conformar o uso das redes pelos menores. Todavia, o projeto de reforma é mais específico e explicita que deve ser garantido um ambiente seguro e saudável para utilização das redes sociais pelas crianças e pelos adolescentes.

Essa proteção integral, na verdade, já se encontrava prevista na Constituição (art. 227) na forma de dever da família, da sociedade e do Estado. A prioridade conferida a esse dever precisa ser absoluta e deve abranger políticas específicas de assistência à saúde, limitações ao trabalho infantil, disponibilização de educação pública de qualidade e inimputabilidade penal até os 18 anos; determinação de elaboração de lei com punição severa a abuso, à violência e à exploração sexual de crianças e adolescentes; igualdade entre filhos, entre outras garantias especiais de caráter processual penal.

No que diz respeito ao ambiente digital, o ECA apenas menciona a inclusão digital, por meio do acesso às novas tecnologias da informação e comunicação quando trata dos direitos à cultura (art. 22) e à comunicação e à liberdade de expressão (art. 27). Não foram tecidas considerações para a limitação desse acesso, nem foram previstas responsabilidades aos agentes do mercado digital.

Por último, no que se refere à primeira infância, compreendendo os seis primeiros anos de vida, a Lei nº 13.257/2016 estabeleceu como áreas prioritárias para as políticas públicas voltadas à valorização da convivência familiar e comunitária, a promoção da cultura, do brincar e do lazer, além da proteção contra qualquer tipo de violência e influência consumista, e a implementação de ações que impeçam a exposição precoce à publicidade mercadológica.

Nesse contexto, o direito à imagem de crianças e adolescentes no ambiente digital é um tema de crescente relevância. A Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas, estabelece que os interesses dos menores de idade devem ser prioridade em todas as decisões que os afetam, incluindo a exposição das próprias imagens. Em se tratando de crianças e adolescentes, essa proteção ganha uma importância ainda maior devido à facilidade de compartilhamento de fotos e vídeos, bem como à vulnerabilidade e à imaturidade inerentes a esse grupo etário. As plataformas digitais têm um papel relevante na proteção dos direitos de imagem de crianças e adolescentes e devem implementar políticas claras e eficazes para compartilhamento de fotos e vídeos, bem como para remoção imediata de conteúdos não autorizados ou indesejados. Trata-se, portanto, de uma necessária conscientização entre pais, educadores, crianças e adolescentes para o exercício de uma cidadania digital que permita um acesso seguro e respeitoso.

Tarcísio Teixeira trata do tema do meio ambiente virtual para crianças e adolescentes com foco em *cyberbullying*, pornografia de vingança, *fake news e detox* digital (Teixeira, 2024). O autor pondera que o direito de acesso ao mundo virtual consiste em uma quinta geração de direitos fundamentais, mas aponta os riscos e problemas que esse acesso é capaz de proporcionar, em especial para o público infantil. Em primeiro lugar, o autor destaca o isolamento social, que decorre da prevalência das relações de comunicação por meios tecnológicos em detrimento das relações interpessoais de forma presencial. A perda de produtividade causada pelo vício em recursos tecnológicos também é um fator

de preocupação geral sob o viés da saúde. Não bastasse isso, o afastamento afetivo nos seios familiares é outra triste constatação, o que leva ao foco nos impactos da tecnologia para crianças e adolescentes.

O *bullying*, que é a agressão psicológica ou física praticada, de forma intencional e repetida, por uma ou mais pessoas contra alguém que possa causar-lhe humilhação ou provocando difamação, é um dos problemas a serem repelidos a partir do dever de proteção integral das crianças e adolescentes. No ambiente digital, essa prática ganha o nome de *cyberbullying*. Há quase dez anos, existe a lei que institui programa de combate à intimidação sistemática, inclusive tratando do tema no Brasil.

O art. 2º, parágrafo único, da Lei nº 13.185/2015, prevê que "Há intimidação sistemática na rede mundial de computadores (*cyberbullying*), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial". Não foram previstas medidas de punição aos intimidadores ou aos estabelecimentos que deixem de cumprir com os deveres de conscientização, prevenção, diagnóstico e combate ao *bullying* e *cyberbullying*.

Young e Abreu (2018) alertam especialmente sobre a vulnerabilidade de crianças e adolescentes com problemas de autoestima e de relacionamento social, já que o mundo dos jogos on-line muitas vezes oferece uma alternativa à relação social tradicional com outros indivíduos, permitindo que modelem a aparência dos personagens da forma que os satisfaria no mundo real. Assim, o jovem acaba por se identificar mais com sua persona digital e se sentir mais acolhido e pertencente à realidade do jogo do que à própria, o que proporciona um conforto que viabiliza um quadro de dependência que, por vezes, pode levar até mesmo a um comportamento errático e violento. Dessa forma, evidencia-se que o projeto de lei está aderido às evidências científicas que apontam os prejuízos que o design orientado à dependência pode proporcionar.

Alessandra Borelli (2022), por outro lado, muito embora reconheça os riscos relacionados ao uso exagerado de videogames por crianças e adolescentes, apresenta outra perspectiva sobre o tema ao destacar que os games podem trazer diversas vantagens quando os responsáveis direcionam e orientam os filhos para o melhor uso dos recursos disponíveis nesse universo. Segundo a autora, quando devidamente controlados pelos responsáveis, os jogos podem estimular o desenvolvimento de habilidades como planejamento estratégico e memória, além de trazerem bons resultados em áreas como a psicologia e o desenvolvimento motor (esse último, especificamente em relação aos games como o *Wii*, que exigem atividade física). Ademais, a autora explica também o movimento da "gamificação", que consiste na integração de elementos dos jogos para o estímulo de comportamentos positivos na realidade, como o desenvolvimento de sistema de pontos para a realização de tarefas escolares e da casa.

A autora ainda pondera que os *games* não seriam o único produto digital direcionado ao vício dos usuários. As redes sociais baseiam-se em algoritmos, que direcionam os conteúdos de acordo com as preferências dos usuários, ao mesmo tempo em que excluem, do padrão de sugestão de conteúdos, aqueles vídeos e aquelas imagens que diferem do posicionamento e da preferência, de forma a estimular que se passe mais tempo on-line. Além disso, o sistema de curtidas e compartilhamentos são desenhados para gerar uma sensação de recompensa e gratificação instantâneas, potencialmente viciante pela facilidade com que se atinge esse sentimento positivo.

Dada a imaturidade cerebral dos menores de vinte anos, eles se apresentam mais suscetíveis a desenvolver a dependência de recursos digitais, não apenas pelo fator biológico, mas também como consequência da fase de desenvolvimento, em que buscam mais intensamente a aprovação de terceiros, com maior propensão ao sofrimento causado por uma baixa autoestima. Assim, mesmo diante dos benefícios possíveis, percebe-se que a proposta de dispositivo do projeto é absolutamente necessária e adequada. De fato, o controle sobre o design desses produtos digitais mostra-se como uma alternativa interessante para combater adversidades da juventude contemporânea.

3.5.2 O tratamento da matéria pelas plataformas digitais

a) Meta

A Meta (2025), em fevereiro de 2025, disponibilizou, no Brasil, a conta de adolescente no Instagram com configurações que incluem proteções, restrições de comunicação e filtros de acesso a conteúdos, como se verifica a seguir:

> Configurações de privacidade e segurança para adolescentes
>
> A Meta está empenhada em proporcionar aos jovens uma experiência mais segura e privada. Temos equipes exclusivas focadas na segurança dos jovens e trabalhamos em estreita colaboração com especialistas para direcionar os recursos que desenvolvemos. Aqui estão algumas das configurações padrão e ferramentas adicionais para adolescentes em nossos apps. Os requisitos de idade podem variar de acordo com o país.
>
> Configurações de privacidade e segurança para adolescentes no Facebook
>
> Configurações padrão do Facebook
>
> Compartilhamento de localização: o compartilhamento de localização está desativado para menores de idade por padrão. Quando um adulto ou menor de idade ativa o compartilhamento de localização, incluímos um indicador consistente como um lembrete de que a pessoa está compartilhando sua localização.

Configurações de privacidade: todos os menores de 16 anos (ou menores de 18 anos em determinados países) terão configurações mais privadas quando entrarem no Facebook. Isso inclui:

- Quem pode ver a lista de amigos deles.
- Quem pode ver as pessoas, páginas e listas que seguem.
- Quem pode ver as publicações nas quais foram marcados nos perfis deles.
- Analisar publicações nas quais foram marcados antes que a publicação apareça no perfil deles.
- Quem pode comentar nas publicações abertas deles.
- Protegemos determinadas informações, como informações de contato de menores de idade, escola e data de nascimento, para que não apareçam na pesquisa pública.

Ferramentas adicionais do Facebook

Gerenciamento de tempo

Lembretes de pausa: os adolescentes verão uma notificação quando passarem 20 minutos no Facebook. Essa notificação solicita que façam uma pausa no uso do app e estabeleçam limites de tempo diários. Esse recurso foi desenvolvido para incentivar o uso significativo e intencional do Facebook pelos adolescentes e incentivá-los a fazer pausas regulares.

Recursos no app

Fornecemos instruções específicas aos menores de idade sobre o que significa publicar algo aberto a todos. Além disso, tomamos providências para lembrar aos menores de que eles só devem aceitar solicitações de amizade de pessoas que conhecem.

Configurações de privacidade e segurança para adolescentes no Messenger

Configurações padrão do Messenger

Temos restrições em vigor que limitam a capacidade dos adultos que usam nossos apps de enviar mensagens a adolescentes com os quais não estão conectados.

Restringimos adultos maiores de 18 anos de iniciar bate-papos privados com adolescentes aos quais não estejam conectados no Instagram e no Messenger.

Ferramentas adicionais do Messenger

Supervisão dos pais

Com a supervisão habilitada, pais, mães ou responsáveis podem:

- Ver quanto tempo o adolescente passa no Messenger.
- Visualizar e receber atualizações sobre a lista de contatos do Messenger do adolescente, bem como as configurações de privacidade e segurança de seus filhos.
- Receber notificação se o adolescente denunciar alguém (se o adolescente decidir compartilhar essa informação).
- Ver quem pode enviar mensagens para seu filho adolescente (apenas amigos, amigos de amigos ou ninguém) e ver se o seu filho adolescente alterar essa configuração.
- Ver quem pode visualizar os Messenger Stories do seu filho adolescente no Messenger e receber uma notificação se essas configurações mudarem.

Recursos no app

Avisos: banners que fornecem dicas sobre como detectar atividades suspeitas e adotar medidas para bloquear, denunciar ou ignorar/restringir alguém quando algo parece estar errado.

Configurações de privacidade e segurança para adolescentes no Meta Quest

Supervisão dos pais

Com a supervisão habilitada, pais, mães ou responsáveis podem:

- Aprovar o download ou a compra que os adolescentes desejam fazer de um app bloqueado por padrão com base na classificação da IARC.
- Bloquear apps específicos para adolescentes, o que impedirá que eles iniciem esses apps. É possível bloquear apps como navegadores da web e apps disponíveis na Loja do Quest.
- Ver todos os apps que pertencem aos adolescentes.
- Receber "Notificações de compra" para saber quando os adolescentes fazem uma compra na VR.
- Ver o tempo de tela no headset por meio do app Oculus para celular. Isso permite saber quanto tempo os adolescentes passam na VR.

- Ver a lista de amigos do Oculus dos adolescentes.
- Bloquear o Link e o Air Link. Isso impedirá que o adolescente acesse o conteúdo do computador no headset Quest.

Configurações de privacidade e segurança para adolescentes do Meta Horizon Worlds

Ferramentas de privacidade e segurança do Meta Horizon Worlds

Ferramentas adicionais do Meta Horizon Worlds

Supervisão dos pais

Com a Supervisão habilitada, pais, mães ou responsáveis podem:

- Ver, ajustar e bloquear recursos de segurança como modo de voz e limites pessoais para adolescentes.
- Veja quem o adolescente segue e quem o segue.
- Veja quais apps o adolescente usou e quanto tempo passou no Meta Quest e no Worlds nos últimos sete dias.
- Permita ou bloqueie o uso de apps, inclusive o Worlds.

Configurações de privacidade e segurança para adolescentes no Instagram

Sobre as configurações de privacidade e segurança para adolescentes no Instagram

No momento, as Contas de Adolescente estão disponíveis apenas em algumas localizações e serão lançadas globalmente no início de 2025. As Contas de Adolescente estão sendo implementadas individualmente. Isso significa que os pais e responsáveis podem ter um filho que tenha uma Conta de Adolescente antes que outros adolescentes também tenham uma.

O Instagram quer proporcionar aos jovens experiências mais seguras e privadas. Temos equipes dedicadas a trabalhar principalmente com a segurança dos jovens. Também colaboramos com especialistas a fim de obter informações para as funcionalidades que desenvolvemos. Aqui estão algumas das configurações padrão e ferramentas adicionais para adolescentes no Instagram. Os requisitos de idade podem variar de acordo com o país.

Configurações padrão do Instagram

Verificação de idade

Exigimos a idade mínima de 13 anos para se cadastrar no Instagram. Para confirmar a idade as pessoas podem fornecer sua data de nascimento, identificação com foto e/ou enviar uma selfie em vídeo. A confirmação da idade é um requisito para todos no Instagram.

Contas privadas

Por padrão, todos os adolescentes com menos de 18 anos têm suas contas configuradas como privadas quando se cadastram no Instagram. Pessoas com contas privadas são capazes de controlar quem pode ver ou interagir com o conteúdo delas. Saiba mais sobre contas privadas no Instagram.

Controles do público

Por padrão desde maio de 2022, quando jovens menores de 18 anos se cadastram no Instagram, as contas que eles não seguem não podem marcá-los, nem mencionar ou usar o conteúdo deles em remixes ou guias do Reels.

Mensagens diretas

Restringimos adultos maiores de 18 anos de iniciar bate-papos privados com adolescentes aos quais não estejam conectados no Instagram e no Messenger.

Proteções contra adultos suspeitos

Desenvolvemos tecnologia que nos permite encontrar contas de adultos que mostraram comportamentos potencialmente suspeitos, como adultos que foram recentemente bloqueados ou denunciados por um jovem. Impedimos que as contas de adultos interajam com contas de adolescentes das seguintes formas:

- Não mostramos contas de adolescentes no Explorar, no Reels ou na seção "Contas sugeridas para você" para esses adultos.
- Caso os adultos encontrem contas de jovens pesquisando seus nomes de usuário, eles não terão a opção de segui-los.
- Esses adultos não podem ver contas de adolescentes quando rolam pela lista de pessoas que curtiram uma publicação.
- Esses adultos não podem ver comentários de adolescentes nas publicações de outras pessoas.
- Esses adultos não podem ver contas de adolescentes ao rolarem pela lista de seguidores de uma conta.
- Se esses adultos seguirem uma conta de adolescente, poderemos enviar uma notificação ao adolescente solicitando que analise e remova o novo seguidor.

- Se esses adultos já estiverem conectados a uma conta de adolescente e enviarem uma mensagem direta para ele, enviaremos um aviso de segurança ao adolescente incentivando-o a agir com cautela. Fornecemos a ele opções para encerrar a conversa, bloquear, denunciar ou restringir o adulto.

Observação: todas as intervenções acima também se aplicam à capacidade das contas de adolescentes de descobrir, pesquisar, visualizar ou interagir com contas de adultos suspeitos.

Controle de conteúdo sensível

O controle de conteúdo sensível permite que as pessoas escolham ver muito ou pouco conteúdo sensível de contas que não seguem. Existem duas opções para os adolescentes: "Padrão" e "Menos". Por padrão, todos os adolescentes no Instagram com menos de 18 anos têm o controle definido para o estado "Menos", exceto se optarem explicitamente por desativá-lo. Os adolescentes com menos de 16 anos precisam da permissão de um dos pais ou responsável para alterar essa configuração de Menos para Padrão.

Isso dificulta para os adolescentes encontrarem conteúdo sensível ou contas potencialmente sensíveis nos espaços Pesquisar, Explorar, Páginas de hashtag, Reels, Recomendações do feed e Contas sugeridas. Saiba mais sobre o controle de conteúdo sensível.

Restrições de conteúdo

Para todos os usuários no Instagram, removemos conteúdos que violam nossas Diretrizes da Comunidade e não recomendamos conteúdos que violam nossas Diretrizes de Recomendação.

Para adolescentes menores de 16 anos, ocultamos determinados conteúdos sensíveis no Instagram mesmo que tenham sido compartilhados por amigos ou pessoas que eles seguem. Por exemplo, conteúdo que discute automutilação e distúrbios alimentares ou que inclui nudez adulta limítrofe. Estamos trabalhando na aplicação dessas políticas para menores de 18 anos nos próximos meses.

Para adolescentes menores de 18 anos, removemos os conteúdos que são analisados e possam ser perturbadores (por exemplo, conteúdo explícito e violento).

Por último, para adolescentes menores de 18 anos, limitamos a visibilidade de certos produtos e serviços restritos incluindo conteúdo relacionado com álcool, tabaco, armas brancas, produtos para perda de peso, procedimentos cosméticos, brinquedos sexuais, produtos para melhorar o desempenho sexual, jogos de azar ou enteógenos.

Ferramentas adicionais do Instagram

Supervisão dos pais

A supervisão é um conjunto de ferramentas e insights que pais, mães e responsáveis podem usar para dar suporte aos seus filhos adolescentes (entre 13 e 17 anos) no Instagram. A supervisão é opcional. Tanto o pai, mãe ou responsável como o adolescente devem concordar em participar. Quando a supervisão é configurada na Central da Família, o pai, mãe ou responsável pode definir limites de tempo, agendar intervalos, ver o tempo que o adolescente passa no Instagram, ver os seguidores do adolescente e quem ele segue, conexões compartilhadas, quem ele bloqueou ou denunciou e ver as seleções de configuração de segurança do adolescente.

Cutucar para mudar de tópico

Em alguns países, os adolescentes menores de 18 anos verão uma notificação com um incentivo para mudar de tópico, caso estejam pesquisando o mesmo tipo de conteúdo no Explorar por um certo tempo. Essa cutucada foi criada para incentivar os adolescentes a descobrir algo novo. (Instagram, [s.d.])

3.5.3 Experiências normativas do direito estrangeiro e transnacional

3.5.3.1 União Europeia

Há quase 30 anos, em 1996, a Comissão Europeia publicou um documento reconhecendo a importância da proteção dos menores no ambiente digital, sob o fundamento de que as plataformas digitais poderiam contribuir, de forma mais ostensiva e mais rápida do que a mídia tradicional, para tornarem-se acessíveis ao público infantojuvenil (*Commission of the European Communities*, 1996). Como medida mais prática, também em 1996, a Comissão propôs medidas específicas essencialmente relacionadas a padrões de tecnologia, filtros de conteúdo, controle parental de acesso e sistemas de rótulos de restrição de idade (Castro; Carthy; O'Reilly, 2022).

A partir desses documentos, uma série de programas foram desenvolvidos até que as instituições europeias lançaram iniciativas mais focadas em cada um dos problemas identificados, como as seguintes:

1) O programa "dotSAFE".

2) O "Safer internet forum", traduzido livremente para "Fórum Internet mais segura", desde 2004, com autoridades legais, representantes da indústria, organizações civis (grupos de proteção infantil, grupos de pais e professores associações e grupos de consumidores) e instituições legislativas.

3) Insafe e INHOPE, referindo-se a uma rede global de linhas diretas para denunciar conteúdo on-line com o objetivo de eliminar o abuso sexual infantil on-line.

4) "EU kids online" que consiste em mapear experiências de crianças online, a fim de avaliar sua segurança e riscos em sites.

5) "Mediappro", que é um projeto de alfabetização midiática.

6) Programa "SIP-Bench", referente às estratégias de controle parental.

7) A celebração do Dia da Internet Mais Segura.

8) A criação do "Fórum de Governança da Internet".

9) O estabelecimento de vários pontos de contato onde as crianças possam ser educadas sobre como navegar com segurança na internet e como combater o cyberbullying e abuso sexual online – Centros de Internet Mais Segura (SICs).

10) A Rede POSCON (Positive Online Content and Services for Children in Europe) – traduzido livremente para "Conteúdos e Serviços de internet positivos para crianças na Europa"

11)A Aliança Europeia de ONGs para a Segurança Infantil Online.

12) O "Net Children Go Mobile", .

13) E o SPIRTO (Self-Produced Images Risk Taking Online), projeto de pesquisa pelo qual são examinados os riscos para os jovens a partir da criação e do compartilhamento de conteúdo sexual no meio digital.

O programa europeu sobre o tema que tem ensejado diversas iniciativas na Europa recentemente é o "*Better Internet for Kids*" (BIK, 2021), que consiste em um centro de pesquisa, práticas, redes de cooperação e uma ampla gama de meios de comunicação e iniciativas de alfabetização.

Ainda no âmbito da União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) estabelece normas para a proteção de dados pessoais, incluindo dados de crianças e reconhece a necessidade de proteger especialmente os dados pessoais das crianças devido à sua vulnerabilidade, como se verifica nos dispositivos legais abaixo

Artigo 8º - Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação

1. Quando for aplicável o artigo 6.o, n.o 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o

consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.

2. Nesses casos, o responsável pelo tratamento envidará todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.

3. O disposto no n.o 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança.

Artigo 12º Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados

1. O responsável pelo tratamento tomará as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.o e 14.o e qualquer comunicação prevista nos artigos 15.o a 22.o e 34.o a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados o solicitar, a informação pode ser prestada verbalmente, desde que a identidade do titular seja comprovada por outros meios.

Artigo 40 - Códigos de conduta

[...]

2. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente regulamento, como por exemplo:

[...]

g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido;

Artigo 57 - Atribuições

1. Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controle, no território respectivo:

[...]

b) Deve promover a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial. (Tradução nossa)

Já a Diretiva de Serviços de Comunicação Audiovisual (União Europeia, 2010) regula a distribuição de conteúdos audiovisuais na União Europeia, incluindo a proteção de crianças contra conteúdos prejudiciais, como se verifica abaixo:

(47) A educação para as mídias visa o desenvolvimento das competências, dos conhecimentos e a compreensão que permitam aos consumidores utilizarem os meios de comunicação social de forma eficaz e segura. As pessoas educadas para as mídias são capazes de fazer escolhas informadas, compreender a natureza dos conteúdos e serviços e tirar partido de toda a gama de oportunidades oferecidas pelas novas tecnologias das comunicações. Estão mais aptas a protegerem-se e a protegerem as suas famílias contra material nocivo ou atentatório. A educação para as mídias deverá por conseguinte ser fomentada em todos os setores da sociedade e os seus progressos deverão ser acompanhados de perto. A Recomendação do Parlamento Europeu e do Conselho, de 20 de Dezembro de 2006, relativa à proteção dos menores e da dignidade humana e ao direito de resposta em relação à competitividade da indústria europeia de serviços audiovisuais e de informação em linha, contém já uma série de medidas suscetíveis de fomentar a educação para as mídias, tais como, por exemplo, a formação contínua de professores e formadores, a aprendizagem específica da Internet destinada às crianças desde a mais tenra idade, incluindo sessões abertas aos pais, ou a organização de campanhas nacionais junto dos cidadãos, envolvendo todos os meios de comunicação social, de modo a divulgar informações sobre a utilização responsável da Internet.

(61) Os fornecedores de serviços de comunicação social sob a jurisdição dos Estados-Membros deverão estar, para todos os efeitos, sujeitos à proibição de difusão de pornografia infantil, nos termos da Decisão-Quadro 2004/68/JAI do Conselho, de 22 de Dezembro de 2003, relativa à luta contra a exploração sexual de crianças e a pornografia infantil. (Tradução nossa)

Já no âmbito da Lei de Serviços Digitais (União Europeia, 2022), há a imposição de uma série de exigências de transparência e cuidado para as plataformas digitais e prevê a ampliação das responsabilidades das plataformas em relação a crianças e adolescentes, como se verifica abaixo:

Artigo 34 - Avaliação dos riscos

1. Os fornecedores de plataformas digitais de grande alcance e de motores de pesquisa on-line de grande alcance devem identificar, analisar e avaliar diligentemente todos os riscos sistêmicos na União decorrentes do uso ou do funcionamento do seu serviço e dos seus sistemas relacionados, incluindo os sistemas algorítmicos, ou decorrentes da utilização dos seus serviços.

Devem efetuar as avaliações de risco até à data de aplicação referida no artigo 33.o, n.o 6, segundo parágrafo, e, posteriormente, pelo menos uma vez por ano, e, em qualquer caso, antes da introdução de funcionalidades suscetíveis de terem um impacto crítico nos riscos identificados nos termos do presente artigo. Esta avaliação dos riscos incidirá especificamente nos seus serviços, será proporcionada aos riscos sistêmicos, tendo em conta a sua gravidade e probabilidade, e incluirá os seguintes riscos sistémicos:

[...];

b) Quaisquer efeitos negativos reais ou previsíveis no exercício dos direitos fundamentais, em particular os direitos fundamentais relativos à dignidade do ser humano consagrado no artigo 1.o da Carta, ao respeito pela vida privada e familiar consagrado no artigo 7.o da Carta, à proteção dos dados pessoais consagrado no artigo 8.o da Carta, à liberdade de expressão e de informação, incluindo a liberdade e o pluralismo dos meios de comunicação social consagrado no artigo 11.o da Carta, e à não discriminação consagrado no artigo 21.o da Carta, ao respeito pelos direitos das crianças consagrado no artigo 24.o da Carta e a um elevado nível de defesa dos consumidores, consagrado no artigo 38.o da Carta;

Artigo 35 - Atenuação de riscos

1. Os fornecedores de plataformas digitais de grande alcance e de motores de pesquisa on-line de grande alcance devem adotar medidas de atenuação razoáveis, proporcionadas e eficazes, adaptadas aos riscos sistémicos específicos identificados nos termos do artigo 34.o, tendo especialmente em conta o impacto de tais medidas nos direitos fundamentais. Estas medidas podem incluir, quando aplicável:

[...]

j) A adoção de medidas específicas para proteger os direitos das crianças, nomeadamente instrumentos de verificação da idade e de controle parental, instrumentos destinados a ajudar os menores a sinalizar abusos ou a obter apoio, conforme adequado. (Tradução nossa)

3.5.3.2 Espanha

A Espanha trata da temática a partir de um conjunto de leis e regulamentos que criam diretrizes para a proteção da presença e da identidade de crianças e adolescentes no ambiente digital. A *Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (Espanha, 2018) implementa o Regulamento Geral de Proteção de Dados (GDPR) na Espanha e inclui disposições específicas para a proteção de menores no ambiente digital, como se verifica no artigo 7, que determina que o consentimento para o processamento de dados pessoais de menores deve ser dado ou autorizado pelos titulares da responsabilidade parental quando o menor tiver menos de 14 anos e no artigo 84, que garante o direito à proteção de dados pessoais de menores e medidas para remoção de conteúdos em caso de prejuízo aos interesses dos menores.

Além disso, a *Ley de Protección Jurídica del Menor* (Espanha, 1996) assegura a salvaguarda dos direitos das crianças e adolescentes, abrangendo também sua identidade e presença no ambiente digital, prevendo:

> Artigo 4.º Direito à honra, à intimidade e à própria imagem
>
> 1.Os menores têm direito à honra, à intimidade pessoal e familiar e à própria imagem. Esse direito também compreende a inviolabilidade do domicílio familiar e da correspondência, assim como o sigilo das comunicações.
>
> 2.A divulgação de informações ou a utilização de imagens ou do nome de menores nos meios de comunicação que possa representar uma intromissão ilegítima em sua intimidade, honra ou reputação, ou que seja contrária aos seus interesses, implicará a intervenção do Ministério Público, que deverá imediatamente adotar as medidas cautelares e de proteção previstas em lei, bem como solicitar as indenizações cabíveis pelos prejuízos causados.
>
> 3.Considera-se intromissão ilegítima no direito à honra, à intimidade pessoal e familiar e à própria imagem do menor qualquer uso de sua imagem ou nome nos meios de comunicação que possa prejudicar sua honra ou reputação, ou que seja contrário aos seus interesses, ainda que haja consentimento do menor ou de seus representantes legais.
>
> 4.Sem prejuízo das ações que possam ser exercidas pelos representantes legais do menor, caberá em todo caso ao Ministério Público o exercício dessas ações, podendo atuar de ofício ou a pedido do próprio menor ou de qualquer pessoa interessada, seja ela física, jurídica ou entidade pública. (Espanha, 1996) (Tradução nossa)[25]

25 No original; "Artículo 4. Derecho al honor, a la intimidad y a la propia imagen.

1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

2. La difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea

Foi lançada, também, a estratégia nacional espanhola de cibersegurança, abrangendo essencialmente áreas relacionadas com a promoção de uma cultura de cibersegurança para todos os cidadãos em geral e com o aumento dos níveis de proteção on-line (Espanha, 2019).

3.5.3.3 Reino Unido

O *Online Safety Act* (Reino Unido, 2023) publicado em 2023 impõe maiores responsabilidades às plataformas digitais acessíveis por crianças e adolescentes, exigindo que adotem o "dever de cuidado", bem como criem mecanismos para identificação e mitigação de riscos com canais para denúncias, bem como incorporem a "segurança por design" como padrão em aplicativos voltados para crianças e adolescentes.

3.5.3.4 Síntese analítica das experiências normativas de direito estrangeiro e transnacional

A garantia da proteção de crianças e adolescentes no ambiente digital é uma tendência em diversos países, com normatizações semelhantes. Verifica-se, portanto, que o Projeto de Lei nº 4, de 2025, segue essas mesmas linhas normativas, complementado as proteções previstas no ECA e na LGPD.

A União Europeia estabelece regras rígidas de proteção de dados, de proibição de publicidade direcionada e de avaliação de riscos específicos para menores. Na mesma linha, a Espanha trata da temática a partir de um conjunto de leis e regulamentos que criam diretrizes para a proteção da presença e da identidade de crianças e adolescentes no ambiente digital.

O Reino Unido, por meio do *Online Safety Act* (2023), estabelece o dever de cuidado das plataformas, com a previsão de medidas preventivas desde o design, de maior controle sobre conteúdos acessíveis a crianças e de canais para denúncias.

3.5.4 Estudos de caso

3.5.4.1 Brasil: ADI 5.631

Recentemente, o Plenário do Supremo Tribunal Federal (STF) julgou constitucional uma lei do Estado da Bahia que proíbe propagandas impressas (cartazes, banners e out-

contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

3. Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

4. Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública".

doors) e não impressas de produtos infantis no espaço físico dos estabelecimentos de educação básica. Por unanimidade, o colegiado julgou improcedente a Ação Direta de Inconstitucionalidade (ADI) 5631, com o entendimento de que a norma estadual visa preservar o espaço e o que se faz nele em termos de educação das crianças e dos adolescentes.

3.5.4.2 Brasil: MPRJ - Procedimento preparatório nº 1.30.001.001561/2016-05

Em outro caso, tratou-se dos *unboxings* feitos por crianças que produzem conteúdo em plataformas de vídeos, a exemplo do *Youtube*, uma das mais populares no Brasil. Por causa disso, convencionou-se chamá-los de "*youtubers* mirins" (Criança e Consumo, 2016). Desde 2016, essa prática tem sido objeto de investigações do Ministério Público de diversos estados. Entre as empresas que foram notificadas em razão de publicidade abusiva, consistente no desenvolvimento de estratégias de comunicação mercadológica direcionadas diretamente a crianças, estão Bic Graphic Brasil Ltda., Biotropic Cosmética Licensing, C&A Modas Ltda., Cartoon Network, Foroni Indústria Gráfica Ltda., A Edutenimento Entretenimentos do Brasil Ltda. (Kidzania), Long Jump – Representação de Brinquedos e Serviços Ltda., Mattel do Brasil Ltda.,Arcos Dourados de Alimentos Ltda. (McDonald's), Pampili Produtos Para Meninas Ltda., Lojas Puket Ltda., Ri Happy Brinquedos S.A., Sistema Brasileiro de Televisão – SBT, Sestini Mercantil Ltda.e Tilibra Produtos de Papelaria Ltda.

A prática investigada consistia na utilização de canais de crianças em redes sociais como *YouTube, Facebook e Instagram* para a divulgação de produtos, promoções e serviços. Assim, considerou-se que as empresas exerceram prática abusiva, pois aproveitam-se da vulnerabilidade das crianças youtubers e espectadoras para alavancar as vendas.

Em 2017, uma empresa do ramo de brinquedos fez uma parceria com o canal de uma *youtuber* infantil para a divulgação da promoção "Você Youtuber Escola *Monster High*", a fim de promover a marca e os produtos da linha *Monster High* (Criança e Consumo, 2017). Conforme relatos do Instituto Alana:

> Para participar, as garotas deveriam gravar e postar vídeos cumprindo desafios publicados pela youtuber. As provas foram divididas em três blocos de quatro vídeos cada, totalizando 12 vídeos inspirados em características de três diferentes *monstrinhas* do desenho – Draculaura, filha do Drácula; a Frankie, filha do Frankstein; e Clawdeen, filha do Lobisomem -.
>
> Conforme as regras da promoção, os desafios consistiriam na criação de visuais ligados à moda feminina infantil como maquiagem, penteado, customização de roupas, entre outros, além de criação de histórias com temas do dia a dia, sugeridos pela youtuber mirim.

A cada semana, uma menina era escolhida vencedora para ganhar uma boneca Monster High licenciada pela Mattel, além de um par de ingressos para evento com a presença da influenciadora digital, realizado no dia 31.10.2016 na sede da empresa.

Para divulgar a promoção, a empresa criou uma página específica na internet. Além disso, houve ampla divulgação pela youtuber em suas redes sociais – blog, Facebook, Twitter e Instagram – e em anúncios no YouTube.

O 'Encontrinho' com a influenciadora mirim, que era um dos prêmios da promoção, foi desenvolvido como uma espécie de formatura, na qual as vencedoras ficavam sentadas em uma sala de aula improvisada dentro das dependências da Mattel em São Paulo e tinham a Julia como professora. O escritório da Mattel foi decorado e preparado para a formatura da 'Escola Monster High' de Youtubers. Havia armários escolares em formato de caixão, assim como no desenho animado, e uma mesa repleta de comidas enfeitadas com a temática do mundo das personagens.

Cada vencedora que chegasse ao escritório da Mattel para participar da "formatura" da 'Escola Monster High', recebia uma fantasia de alguma das *monstrinhas* do desenho. Além da roupa, as meninas também foram maquiadas como as personagens. Durante a cerimônia de "formatura", as vencedoras vestiram, por cima da fantasia, uma beca com um chapéu. Elas fizeram um juramento e receberam um certificado assinado pela Julia Silva. Cada vencedora ganhou, também, uma mochila contendo produtos variados, todos licenciados da marca e estampados com desenhos das bonecas.

Como se pode perceber, a promoção aproveitava-se da hipervulnerabilidade do público infantil, que é muito mais suscetível de ser influenciado pelas peças publicitárias e não possui capacidade de discernir e identificar que está sendo alvo de estratégias de persuasão tão eficazes. Assim, a prática conflita com o dever geral de proteção integral das crianças e dos adolescentes. Em 2020, novamente o MPRJ instaurou inquérito civil em razão de práticas similares, que podem ser consideradas trabalho infantil artístico, o qual é regulamentado e deve garantir que os direitos da personalidade dos "*youtubers* mirins" sejam respeitados (Criança e Consumo, 2016).

Na mais recente rede social, que rapidamente se popularizou especialmente entre as crianças e os adolescentes, o *TikTok* trouxe outra forma de exploração de publicidade com foco no público infantil, as "*publicitoks*", conteúdos que não se apresentam como peças de publicidade explicitamente, mas que veiculam conteúdo eminentemente mercadológico. Por trás desses conteúdos, está o uso e manejo dos dados pessoais dos usuários do aplicativo, incluídas as crianças, o que leva, também, a questionamentos quanto à legitimidade desse fluxo de atividades.

3.5.5 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.5.5.1 Resolução CONANDA nº 245/2024

A Resolução nº 245, de 5 de abril de 2024, elaborada pelo CONANDA (Conselho Nacional dos Direitos da Criança e do Adolescente), aborda os direitos de crianças e adolescentes no contexto digital, a partir de princípios, recomendações e obrigações para as entidades dos setores público e privado. O documento estabelece princípios fundamentais para a proteção dos direitos de crianças e adolescentes no contexto digital, incluindo:

> Art. 3º A garantia e efetivação dos direitos da criança e do adolescente em ambiente digital é pautada pelos seguintes princípios:
>
> I – Não discriminação;
>
> II – Prevalência, primazia e precedência do superior interesse e dos direitos da criança e do adolescente;
>
> III – Direito à vida, à sobrevivência e ao desenvolvimento físico, mental, moral, espiritual e social;
>
> IV – Respeito à liberdade de expressão e de consciência, ao acesso à informação, à autonomia progressiva e à escuta e participação da criança e do adolescente;
>
> V – O livre desenvolvimento da personalidade, da dignidade, da honra e da imagem;
>
> VI – A promoção de um ambiente digital saudável e seguro, livre de assédio, discriminação e discursos de ódio;
>
> VII – O estímulo ao uso consciente e responsável para o exercício da cidadania em ambientes digitais;
>
> VIII – A proteção de dados, a autodeterminação informativa e a privacidade.
>
> IX – A proteção contra toda forma de negligência, discriminação, violência, crueldade, opressão e exploração, inclusive contra a exploração comercial.
>
> X – A garantia dos direitos das crianças e adolescentes por design dos produtos e serviços em ambientes digitais.

Além disso, institui a "política nacional de proteção dos direitos da criança e do adolescente no ambiente digital"; trata da liberdade de expressão de crianças e adolescentes, bem como do direito à privacidade e proteção de dados no ambiente digital; do dever de cuidado e das responsabilidades das empresas provedoras de produtos e serviços digitais; das ações de mobilização e conscientização sobre o impacto do ambiente digital para crianças e adolescentes.

3.5.5.2 São Paulo: Leis Estaduais nº 12.730/2007 e nº 18.058/2024

Desde 2007, está em vigor a Lei Estadual (SP) nº 12.730/2007, que proíbe o uso telefone celular nos estabelecimentos de ensino do Estado, durante o horário de aula, com alterações relevantes realizadas pela Lei Estadual (SP) nº 18.058/2024, que incluiu outros dispositivos eletrônicos, tais como relógios inteligentes e tablets e amplia o horário de proibição para incluir intervalos e atividades extracurriculares. Há permissão de uso dos dispositivos digitais como ferramentas pedagógicas específicas ou sem caso de alunos com deficiência que precisem de auxílio tecnológico.

3.5.5.3 Lei nº 15.100/2025

No mesmo sentido da legislação estadual de São Paulo, a Lei Federal nº 15.100/2025 veda o uso de celulares e aparelhos eletrônicos portáteis aos alunos das escolas públicas e privadas durante as aulas e intervalos.

3.5.6 Comentários sobre o texto do projeto da reforma do Código Civil

Apesar das contribuições normativas do ECA e da LGPD, ambos os diplomas se mostram ainda limitados diante dos novos riscos que emergem no ambiente digital. O ECA mantém-se voltado sobretudo à proteção contra perigos físicos tradicionais, enquanto a LGPD ainda depende, em grande medida, do consentimento dos pais como mecanismo central de controle, o que se torna insuficiente frente à complexa assimetria informacional que caracteriza o tratamento de dados de crianças e adolescentes. Desta forma, o Art 2.027-AH estabelece que "[é] garantida a proteção integral de crianças e adolescentes no ambiente digital, observado o seu melhor e superior interesse, nos termos do estatuto que os protege e deste Código, estabelecendo-se, no ambiente digital, um espaço seguro e saudável para sua utilização".

Já o Art. 2.027-AI do projeto de reforma do Código Civil estabelece as seguintes obrigações aos provedores de serviços digitais: a) implementar sistemas eficazes de verificação da idade dos usuários para assegurar que crianças e adolescentes não acessem conteúdos inapropriados; b) oferecer meios para que pais e responsáveis possam efetivamente limitar e monitorar o acesso de crianças e adolescentes a determinados conteúdos e funcionalidades no ambiente digital; c) garantir a proteção dos dados pessoais de crianças e adolescentes conforme a Lei nº 13.709, de 14 de agosto de 2018; d) assegurar a proteção dos direitos das crianças e adolescentes desde a concepção do ambiente digital, garantindo que, em todas as fases de desenvolvimento, oferta, regulação, gestão de comunidades, comunicação e promoção de seus produtos e serviços, o interesse superior das crianças e adolescentes seja priorizado.

Todas essas obrigações estão alinhadas com as Diretrizes para a Indústria sobre Proteção Infantil On-line, elaboradas pela União Internacional de Telecomunicações (UIT) e

traduzidas para o português por meio de uma parceria entre a Anatel, a Embaixada do Reino Unido e o Comitê Gestor da Internet (CGI.br) (Anatel, 2020). No referido material, as diretrizes gerais de proteção das crianças no ambiente on-line são as seguintes:

i. Integrar os direitos da criança em todas as políticas corporativas e processos de gestão adequados;

ii. Desenvolver padrões da indústria para proteger as crianças on-line;

iii. Desenvolver processos padrão para material de pornografia infantil;

iv. Criar um ambiente on-line mais seguro e apropriado à faixa etária;

v. Educar filhos, pais e educadores sobre a segurança das crianças e seu uso responsável de TICs;

vi. Usar avanços tecnológicos para proteger e educar crianças;

vii. Promover a tecnologia como ferramenta para reforçar ainda mais o engajamento cívico;

viii. Investir em pesquisa.

O Art. 2.027-AK do projeto da reforma trata da vedação à publicidade infantil. Nesse ponto, o projeto vai além da proteção que decorre do texto, já positivado no CDC (Lei nº 8.078/1990) e no ECA, na parte relacionada à publicidade infantil, aproximando-se da Resolução CONANDA nº 163/2016. Estabelece, ainda, a proibição da inclusão de publicidade em qualquer produto ou serviço de tecnologia da informação direcionado a crianças e adolescentes, mesmo que seja gratuito, abrangendo plataformas de compartilhamento de vídeo, redes sociais e outros produtos ou serviços de tecnologia da informação.

O Art. 2.027-AJ do projeto da reforma prevê que produtos e serviços de tecnologia da informação destinados a crianças e adolescentes devem ser criados, projetados, desenvolvidos, disponibilizados, comercializados, disseminados, compartilhados, transmitidos e operados com o intuito de garantir a proteção total e o atendimento prioritário aos seus interesses.

Além disso, os desenvolvedores dos produtos ou serviços referidos no caput deste artigo são obrigados a: a) levar em conta os direitos, capacidades e limitações das crianças e adolescentes a que se destinam, desde a concepção e o projeto, e durante a execução, disponibilização e uso, adotando opções que maximizem a proteção da privacidade e reduzam a coleta e utilização de dados pessoais por padrão; b) empregar uma linguagem clara, concisa, compreensível e adequada, compatível com a idade das crianças e adolescentes a que se destinam; c) assegurar a privacidade e segurança das crianças e adolescentes, em conformidade com seu estatuto e este Código, bem como os demais direitos garantidos pela Constituição Federal, e por Tratados e Convenções assinados pelo Brasil, como a Convenção sobre os Direitos da Criança das Nações Unidas.

Enquanto o CDC prevê que se configura como publicidade abusiva a que se aproveite

da deficiência de julgamento e experiência da criança ou seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua vida ou segurança (art. 37, §2º), o ECA, sem tratar especificamente de publicidade e propaganda, prevê no art. 76, *caput*, que as emissoras de rádio e televisão somente poderão exibir programas com finalidades educativas, artísticas, culturais e informativas no horário recomendado para o público infantojuvenil.

A referida Resolução nº 163 do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA) concretiza e especifica a proteção ao público infantil. Dispõe, por exemplo, que por "comunicação mercadológica" deve-se entender por qualquer atividade de comunicação comercial, incluindo, mas não se limitando à publicidade, para a divulgação de produtos, serviços, marcas e empresas independentemente do suporte, da mídia ou do meio utilizado.

O projeto de lei, ao ressaltar que os dados das crianças e dos adolescentes devem ser tratados na forma da Lei Geral de Proteção de Dados (LGPD), atrai a análise do que dispõe o art. 14 dessa lei tão importante e inovadora. Dada a relevância, reproduz-se a seção pertinente à proteção e dados infantis:

> CAPÍTULO II – DO TRATAMENTO DE DADOS PESSOAIS
>
> (...)
>
> Seção III
>
> Do Tratamento de Dados Pessoais de Crianças e de Adolescentes
>
> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras ativi-

dades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Como visto, o projeto de lei destaca o dever dos provedores de serviços digitais de proteger os interesses da criança e do adolescente desde o design do ambiente digital. A doutrina (Young; Abreu, 2018) tem investigado os impactos da dependência por jogos on-line que tem acometido um número cada vez maior de crianças e adolescentes. Essa dependência tem sido atribuída, entre outros, ao próprio design desses programas. Os especialistas alertam sobre o desenvolvimento dos videogames, que são direcionados justamente para capturar a atenção do jogador na intenção de aumentar a quantidade de tempo conectado ao jogo.

3.6 Inteligência artificial

O texto abaixo está contido no Capítulo VII do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Inteligência artificial".

CAPÍTULO VII

INTELIGÊNCIA ARTIFICIAL

Art. 2027-AL. O desenvolvimento de sistemas de inteligência artificial deve respeitar os direitos de personalidade previstos neste Código, garantindo a implementação de sistemas seguros e confiáveis, em benefício da pessoa natural ou jurídica e do desenvolvimento científico e tecnológico, devendo ser garantidos:

I - a não discriminação em relação às decisões, ao uso de dados e aos processos baseados em inteligência artificial;

II - condições de transparência, auditabilidade, explicabilidade, rastreabilidade, supervisão humana e governança;

III – a acessibilidade, a usabilidade e a confiabilidade;

IV – a atribuição de responsabilidade civil, pelo princípio da reparação integral dos danos, a uma pessoa natural ou jurídica em ambiente digital.

Parágrafo único. O desenvolvimento e o uso da inteligência artificial e da robótica em áreas relevantes para os direitos de personalidade devem ser monitorados pela sociedade e regulamentados por legislação específica.

Art. 2027-AM. Pessoas naturais que interagirem, por meio de interfaces, com sistemas de inteligência artificial, incorporados ou não em equipamentos, ou que sofrerem danos decorrentes da operação desses sistemas ou equipamentos, têm o direito à informação sobre suas interações com tais sistemas, bem como sobre o modelo geral de funcionamento e critérios para decisão automatizada, quando esta influenciar diretamente no seu acesso ou no exercício de direitos, ou afetar seus interesses econômicos de modo significativo.

Art. 2027-AN. É permitida a criação de imagens de pessoas vivas ou falecidas, por meio de inteligência artificial, para utilização em atividades lícitas, desde que observadas as seguintes condições:

I – obtenção prévia e expressa de consentimento informado da pessoa ou dos herdeiros legais ou representantes do falecido;

II – respeito à dignidade, à reputação, à presença e ao legado da pessoa natural, viva ou falecida, cuja imagem é digitalmente representada, evitando usos que possam ser considerados difamatórios, desrespeitosos ou contrários ao seu modo de ser ou de pensar, conforme externado em vida, por seus escritos ou comportamentos ou por quaisquer outras formas pelas quais a pessoa se manifestou ou se manifesta, de natureza cultural, religiosa ou política;

III – para que se viabilize o uso comercial da criação a respeito de pessoa falecida, prévia e expressa autorização de cônjuges, de herdeiros ou de seus representantes ou por disposição testamentária;

IV – absoluto respeito a normas cogentes ou de ordem pública, sobretudo as previstas neste Código e na Constituição Federal.

§ 1º A criação de imagens de pessoas vivas ou falecidas para fins de exploração comercial sem o consentimento expresso da pessoa natural viva ou, caso falecida, dos herdeiros ou representantes legais é proibida, exceto nos casos previstos em lei.

§ 2º As imagens criadas estão sujeitas às leis de direitos autorais e à proteção da imagem, sendo os herdeiros legais ou representantes do falecido os titulares desses direitos.

§ 3º Em todas as imagens criadas por inteligência artificial, é obrigatória a menção de tal fato em sua veiculação, de forma clara, expressa e precisa.

§ 4º Aplicam-se, no que couber, os direitos aqui estabelecidos aos avatares e a outros mecanismos de exposição digital das pessoas jurídicas.

3.6.1 Abordagem teórica da temática

A Ipsos conduziu uma pesquisa para o Google cujos resultados foram divulgados em um relatório intitulado "*Our life with AI: from innovation to application*", com o público de 21 países, focando as experiências e expectativas em relação ao futuro da IA (Google; Ipsos, 2025). Os dados indicam um aumento no uso de IA globalmente e apontam um otimismo crescente quanto ao seu potencial em melhorar a vida das pessoas. A pesquisa foi realizada entre 17 de setembro e 8 de outubro de 2024. Durante esse período, cerca de 21.043 adultos, todos com mais de 18 anos, foram entrevistados on-line nos seguintes países: África do Sul, Alemanha, Austrália, Bélgica, Brasil, Canadá, Chile, Cingapura, Coreia do Sul, Emirados Árabes Unidos, Espanha, Estados Unidos, França, Holanda, Índia, Itália, Japão, México, Nigéria, Polônia e Reino Unido.

No Brasil, de acordo com os dados do estudo, 54% dos brasileiros afirmaram ter utilizado essas ferramentas em 2024 e 65% mostraram confiança no potencial da tecnologia. A pesquisa destacou ainda o impacto da inteligência artificial no mercado de trabalho. No Brasil, 60% dos participantes acreditam que a IA tem o potencial de criar mais empregos, enquanto esse número é de 49% globalmente (Moraes, 2025).

A pesquisa também revelou que, no Brasil, a inteligência artificial está sendo aplicada em áreas além do entretenimento, como ciência (80%), medicina (77%) e agricultura (74%). De acordo com o levantamento, 81% dos brasileiros usam a tecnologia para pesquisas on-line, 78% para assistentes de escrita e 74% a consideram um recurso educacional relevante.

O uso da inteligência artificial na geração de imagens é uma área em crescimento. A capacidade de criar imagens extremamente realistas pode ser utilizada para permitir a circulação da imagem de uma pessoa mesmo após a sua morte, com interações que

podem não estar de acordo com valores e crenças que a pessoa tinha em vida[26]. Por outro lado, como ressalta Laura Porto (2025a), algumas pessoas consideram esses recursos como uma conexão entre gerações, atuando como uma forma de homenagem e preservação da memória afetiva (Ortega, 2024).

Embora a geração de imagens por IA ofereça muitas oportunidades criativas, também levanta questões éticas, como o potencial para criar *deepfakes*[27] ou imagens enganosas (Souza, 2025) que podem ser usadas para desinformação[28].

As *deepfakes* podem se manifestar de várias maneiras, usando diferentes técnicas que permitem uma variedade de truques computacionais[29]: substituição de um rosto por outro *(face-swap*, ou troca de face); clonagem de voz, aparência e gestos, criando um vídeo em que a pessoa replicada imita todas as falas e todos os movimentos do ator (*pupper-master*, ou jogo do ventríloquo); modificação da área da boca para sincronizar o movimento dos lábios com um áudio adicionado (lip-sync, ou sincronização labial).

A IWF (*Internet Watch Foundation*) encontrou imagens de abusos sexuais infantojuvenis produzidas com o uso de inteligência artificial (IWF, 2023). O relatório produzido pela IWF indica que, no decorrer de um mês, foram publicadas 20.254 imagens criadas por IA em um fórum da *dark web*. Dessas, 11.108 imagens foram escolhidas para análise

26 Imagine abrir o celular, entrar em uma rede social e se deparar com a imagem de alguém que você ama, falecido há anos, sorrindo, cantando ou vendendo um produto. Não se trata de uma lembrança antiga, mas de algo novo, atual e vívido. Em outro cenário, é a sua própria imagem que aparece realizando ações que você nunca fez, promovendo uma marca que você nunca consumiu ou apoiando um candidato político ao qual você jamais se filiou. A princípio, tudo parece real, o rosto, os gestos, até a entonação da voz. Só mais tarde, você descobre que aquilo não é uma gravação antiga, nem uma montagem grosseira, mas sim, uma imagem criada por inteligência artificial". (Porto, 2025a)

27 "A expressão "deepfake" surge da união dos termos "deep" – extraída da tecnologia deep learning, "aprendizado profundo" – e "fake", que significa "falso", em inglês. Não existe uma palavra em português para descrever esse fenômeno. Contudo, em tradução livre as deepfakes nada mais são do que "falsidades profundas", ou seja, conteúdos falsos produzidos com um alto grau de elaboração. No caso das deepfakes, a inteligência artificial é usada para gerar imagens, áudios ou vídeos fraudulentos, a partir da adulteração de elementos visuais (troca de rostos, modificação do local, transformação da aparência), auditivos (substituição ou sobreposição de vozes, invenção de diálogos) ou audiovisuais preexistentes, de forma a fazer com que as pessoas acreditem na existência de algo que não ocorreu. Em outros casos, as falsidades profundas surgem da aplicação de ferramentas generativas para a geração de registros fotográficos, áudios ou vídeos totalmente artificiais a partir de comandos específicos". (Brasil. Guia Ilustrado Contra as Deepfakes, 2024)

28 "Na Índia, por exemplo, campanhas políticas utilizaram a voz de líderes mortos para pedir votos, recriando discursos como se fossem atuais. Na Indonésia, a imagem de um político influente, falecido há anos, foi reconstruída digitalmente para aparecer em vídeo apoiando um candidato nas eleições. Ou o famoso caso ocorrido em New Hampshire, onde eleitores receberam ligações com a voz do Presidente Biden, pedindo que estes não saíssem para votar. Esses episódios revelam um uso da tecnologia que ultrapassa os limites da homenagem ou da lembrança, trata-se de um reposicionamento forçado de pessoas em contextos que elas nunca autorizaram, com consequências reais sobre memória, reputação e até mesmo podendo ter influência no debate público." (Porto, 2025a)

29 "As *deepfakes* mais sofisticadas são produzidas com o uso de redes generativas adversárias (também conhecidas como GANs, GENERATIVE ADVERSARIAL NETWORKS). Em uma GAN, dois algoritmos competem entre si: o primeiro com a função de gerar conteúdos falsos indetectáveis, e o segundo com a função de descobrir e apontar as falhas do primeiro. Dessa maneira, o primeiro algoritmo é constantemente aprimorado, conseguindo produzir resultados cada vez mais reais. Em alguns casos, contudo, utilizam-se técnicas menos complicadas, como a simples redução da velocidade de fala para fazer parecer que o sujeito está bêbado. Nessas hipóteses, os vídeos adulterados recebem o nome de "cheapfakes", por constituírem "falsificações baratas", menos sofisticadas do que as "deepfakes" (Brasil. Guia Ilustrado Contra as Deepfakes, 2024, p. 8).

por especialistas da IWF, sendo consideradas as mais prováveis de serem criminosas. As restantes 9.146 imagens geradas por IA ou não continham crianças ou não apresentavam conteúdo de natureza criminosa. Um grupo de 12 analistas da IWF dedicou um total de 87,5 horas para avaliar essas 11.108 imagens criadas por IA e concluiu que 2.562 imagens foram avaliadas como pseudofotografias criminosas e 416 avaliadas como imagens proibidas criminalmente.

As normas do Código Civil em vigor foram criadas a partir de um cenário analógico, no qual a geração de imagens por IA não era ainda possível. Desta forma, as normas em vigor sobre imagem, privacidade e personalidade não estão aptas a dar conta de questões como simulação de imagens, incluindo as *deepfakes*. Desta forma, a previsão de um capítulo sobre inteligência artificial no Livro Direito Civil Digital preenche uma importante lacuna do ordenamento jurídico brasileiro.

3.6.2 O tratamento da matéria pelas plataformas digitais

a) Google

O Google publicou, em 2024, com o objetivo de promover maior transparência no ambiente digital, uma nova diretriz para identificar imagens produzidas ou modificadas por inteligência artificial nos resultados de busca, além de disponibilizar uma "política de uso proibido da IA generativa" (Google, 2024).

> POLÍTICA DE USO PROIBIDO DA IA GENERATIVA
>
> Os modelos de IA generativa podem ajudar você a aprender, entender e criar. Esperamos que você interaja com eles de maneira responsável, legal e segura. As restrições abaixo se aplicam às suas interações com a IA generativa nos produtos e serviços do Google que se referem a esta política.
>
> Não participe de atividades perigosas ou ilegais, nem viole leis ou regulamentações aplicáveis. Isso inclui gerar ou distribuir conteúdo que:
>
> Esteja relacionado a abuso ou exploração sexual infantil.
>
> Facilite o extremismo violento ou o terrorismo.
>
> Facilite imagens íntimas não consensuais.
>
> Facilite a automutilação.
>
> Facilite atividades ilegais ou violações da lei, como fornecer instruções para sintetizar ou ter acesso a substâncias, produtos ou serviços ilegais ou regulamentados.
>
> Viole os direitos de outras pessoas, incluindo privacidade e direitos de propriedade intelectual, por exemplo, o uso de dados pessoais ou biometria sem consentimento legalmente exigido.

Rastreie ou monitore pessoas sem o consentimento delas.

Tome decisões automatizadas que têm um impacto prejudicial significativo nos direitos individuais sem supervisão humana em domínios de alto risco, por exemplo, em áreas jurídicas, de empregos, saúde, finanças, habitação, seguros ou bem-estar social.

Não comprometa a segurança de outros usuários ou dos serviços do Google. Isso inclui gerar ou distribuir conteúdo que facilite:

Spam, phishing ou malware.

Abuso, dano, interferência ou interrupção de serviços ou infraestrutura do Google ou de terceiros.

Evasão de proteções contra abuso ou filtros de segurança, por exemplo, manipular o modelo para violar nossas políticas.

Não se envolva em atividades sexualmente explícitas, violentas, de ódio ou nocivas. Isso inclui gerar ou distribuir conteúdo que facilite:

Ódio ou discurso de ódio.

Assédio, bullying, intimidação, abuso ou insulto a outras pessoas.

Violência ou incitação à violência.

Conteúdo sexualmente explícito, como pornografia ou de satisfação sexual.

Não se envolva em atividades de desinformação, deturpação ou enganosas. Isso inclui:

Fraudes, golpes ou outras ações enganosas.

Falsificação da identidade de um indivíduo (vivo ou morto) sem divulgação explícita da imitação com o objetivo de enganar o público.

Facilitação de declarações enganosas de experiência ou especialidade em áreas sensíveis, como saúde, finanças, serviços públicos ou jurídicos.

Facilitação de declarações enganosas relacionadas a processos governamentais ou democráticos ou práticas de saúde prejudiciais.

Deturpação da procedência de um conteúdo ao declarar que ele foi criado inteiramente por um ser humano, para enganar o público.

Podemos abrir exceções a essas políticas com base em considerações educacionais, documentais, científicas ou artísticas, ou quando os danos são compensados por benefícios significativos para o público. (Google, 2024)

b) Meta

Em 2024, a Meta, empresa que engloba Facebook, Instagram e Threads, publicou alterações nas próprias diretrizes para mídias criadas e modificadas digitalmente, que desafiarão a habilidade dessa rede de monitorar um conteúdo enganoso, produzido por novas tecnologias de inteligência artificial:

> Estamos fazendo mudanças na maneira como lidamos com a mídia manipulada com base no feedback do Conselho de Supervisão e em nosso processo de revisão de políticas com pesquisas de opinião pública e consultas de especialistas.
>
> Começaremos a adicionar rótulos de "informações de IA" a uma gama mais ampla de conteúdo de vídeo, áudio e imagem quando detectarmos indicadores de imagem de IA padrão da indústria ou quando as pessoas divulgarem que estão enviando conteúdo gerado por IA. (Atualizado em 1 de julho de 2024 para refletir o rótulo revisado)
>
> Concordamos com a recomendação do Conselho de Supervisão de que fornecer transparência e contexto adicional agora é a melhor maneira de abordar a mídia manipulada e evitar o risco de restringir desnecessariamente a liberdade de expressão, portanto, manteremos esse conteúdo em nossas plataformas para que possamos adicionar rótulos e contexto. (Meta, 2024)

3.6.3 Experiências normativas do direito estrangeiro e transnacional

3.6.3.1 União Europeia

O *AI Act* de 2024 impõe que os provedores de serviços informem os usuários quando eles estiverem lidando com conteúdo gerado por inteligência artificial, especialmente se esse conteúdo for "semelhante de forma apreciável a pessoas, objetos, lugares, entidades ou eventos existentes" (União Europeia, 2024b), no mesmo sentido da regulamentação apresentada no Projeto de Lei nº 4, de 2025.

> Artigo 50: Obrigações de transparência para provedores e responsáveis pela implantação de determinados sistemas de inteligência artificial
>
> 1. Os provedores devem garantir que os sistemas de IA destinados a interagir diretamente com pessoas físicas sejam projetados e desenvolvidos de tal forma que as pessoas físicas envolvidas sejam informadas de que estão interagindo com um sistema de IA, a menos que isso seja óbvio do ponto de vista de uma pessoa física razoavelmente bem-informada, observadora e advertida, levando em consideração as circunstâncias e o contexto de uso. Esta obrigação não se aplica a sistemas de IA autorizados por lei para detectar, prevenir, investigar ou

processar infrações penais, sujeitas a salvaguardas apropriadas para os direitos e liberdades de terceiros, a menos que esses sistemas estejam disponíveis para que o público denuncie uma ofensa criminal.

2. Os provedores de sistemas de IA, incluindo sistemas de IA de uso geral, que gerem conteúdo sintético de áudio, imagem, vídeo ou texto, devem garantir que os resultados do sistema de IA sejam marcadas em um formato legível por máquina e detectáveis como geradas ou manipuladas artificialmente. Os provedores devem garantir que suas soluções técnicas sejam eficazes, interoperáveis, robustas e confiáveis na medida em que isso seja tecnicamente viável, levando em consideração as especificidades e limitações de vários tipos de conteúdo, os custos de implementação e o estado da arte geralmente reconhecido, como pode ser refletido nos padrões técnicos relevantes. Esta obrigação não se aplicará na medida em que os sistemas de IA desempenhem uma função de assistência para edição padrão ou não alterem substancialmente os dados de entrada fornecidos pelo implantador ou sua semântica, ou quando autorizado por lei para detectar, prevenir, investigar ou processar infrações penais.

[...]

4.Os responsáveis pela implantação de um sistema de IA que gere ou manipule conteúdo de imagem, áudio ou vídeo que constitua uma falsificação profunda, devem revelar que o conteúdo foi gerado ou manipulado artificialmente. Esta obrigação não se aplicará quando o uso for autorizado por lei para detectar, prevenir, investigar ou processar infrações penais. Quando o conteúdo faz parte de um trabalho ou programa evidentemente artístico, criativo, satírico, ficcional ou análogo, as obrigações de transparência estabelecidas neste parágrafo estão limitadas à divulgação da existência de tal conteúdo gerado ou manipulado de maneira apropriada que não impeça a exibição ou a fruição do trabalho.

Os responsáveis pela implantação de um sistema de IA que gere ou manipule texto publicado com o objetivo de informar o público sobre questões de interesse público devem revelar que o texto foi artificialmente gerado ou manipulado. Esta obrigação não se aplica se a utilização for autorizada por lei para detectar, prevenir, investigar e reprimir infrações penais ou se os conteúdos gerados por IA tiverem sido objeto de um processo de análise humana ou de controle editorial e se uma pessoa singular ou coletiva for responsável editorial pela publicação do conteúdo. (Tradução nossa)

Além desses diplomas normativos, a UE publicou a Diretiva (UE) 2024/1385 pelo Parlamento Europeu e pelo Conselho, estabelecendo normas para a criminalização de certas formas de violência doméstica e contra as mulheres. Uma das principais novidades para o ambiente digital é a exigência de que os países-membros criminalizem a criação e distribuição de *deepfakes* com conteúdo sexual sem consentimento, como se verifica no artigo 5º:

Partilha não consensual de material íntimo ou manipulado

1. Os Estados-Membros asseguram que os seguintes comportamentos intencionais sejam puníveis como crime:

a) Divulgação ao público, através das tecnologias da informação e da comunicação (TIC), de imagens, vídeos ou materiais semelhantes que representem atos sexualmente explícitos ou as partes íntimas de uma pessoa, sem o consentimento dessa pessoa, sempre que esse comportamento seja suscetível de causar danos graves a essa pessoa;

b) Produzir, manipular ou adulterar e, subsequentemente, disponibilizar publicamente, através das TIC, imagens, vídeos ou materiais semelhantes, dando a ideia de que uma pessoa participa em atos sexualmente explícitos, sem o consentimento dessa pessoa, sempre que esse comportamento seja suscetível de causar danos graves a essa pessoa;

c) Ameaçar adotar os comportamentos referidos nas alíneas a) ou b), a fim de coagir uma pessoa a praticar, tolerar ou abster-se de um determinado ato.

2. O n.o 1, alíneas a) e b), do presente artigo não afeta a obrigação de respeitar os direitos, as liberdades e os princípios consagrados no artigo 6.o do TUE e aplica-se sem prejuízo dos princípios fundamentais relacionados com a liberdade de expressão e de informação e a liberdade das artes e das ciências, tal como transpostos para o direito da União ou para o direito nacional. (Tradução nossa) (União Europeia, 2024a)

3.6.3.2 Austrália

A emenda ao Código Penal de 2024 (*Deepfake Sexual Material*) introduz a previsão de novas infrações penais destinadas a proibir a distribuição sem consentimento de pornografia produzida por inteligência artificial ou outra tecnologia (Austrália, 2024). As sanções são rigorosas, prevendo até seis anos de prisão pelo ato de compartilhar esse tipo de conteúdo, e até sete anos para aqueles que o criem e compartilhem. O objetivo da legislação é combater o uso nocivo de conteúdo digitalmente gerado, frequentemente empregado para degradar e humilhar principalmente mulheres e meninas.

3.6.3.3 China

A China publicou as "Disposições Administrativas da China sobre Síntese Profunda em Serviços de Informação Baseados na Internet", em 2023, por meio da Administração do Ciberespaço da China (CAC). Esta lei determina que sejam aplicadas pequenas etiquetas por marca d'água dispostas num dos cantos da imagem informando sobre o uso de inteligência artificial (China, 2023).

3.6.3.4 Estados Unidos

Como já visto anteriormente, nos Estados Unidos, 21 estados americanos já promulgaram pelo menos uma lei que criminaliza ou estabelece a responsabilidade civil em razão da disseminação de *deepfakes* em plataformas digitais, havendo atualmente 50 leis já promulgadas (Public Citizen Tracker, 2024). Não há acordo semântico ou uniformidade sobre o tema entre as legislações estaduais.

3.6.3.5 Síntese analítica das experiências normativas de direito estrangeiro e transnacional

A criminalização da produção e da divulgação de *deepfakes* não consensuais foi estabelecida pela Austrália e pela União Europeia. O Reino Unido embora proíba o compartilhamento de *deepfakes* pornográficos sem consentimento, não criminaliza sua criação de forma autônoma.

A China e a União Europeia exigem marcações visíveis em conteúdos gerados por IA, no mesmo sentido do Projeto de Lei nº 4, de 2025. Além disso, o Projeto de Lei nº 4, de 2025, impõe o consentimento prévio para o uso da imagem de pessoas vivas ou falecidas, bem como estabelece deveres de transparência e supervisão humana nas decisões automatizadas e assegura o direito à informação sobre os critérios utilizados por sistemas de I.A, aproximando-se conceitualmente dos modelos internacionais de proteção da personalidade frente aos riscos da IA.

3.6.4 Estudos de caso

3.6.4.1 Brasil: Caso Elis Regina

Uma campanha comemorativa dos 70 anos da Volkswagen do Brasil gerou reclamações de consumidores no conselho de ética do Conselho Nacional de Autorregulamentação Publicitária (Conar) e teve grande repercussão na imprensa e nas redes sociais – com opiniões tanto positivas quanto negativas. Isso ocorreu devido ao uso de inteligência artificial generativa híbrida para recriar a imagem da cantora Elis Regina, falecida em 1982, cantando a música *Como nossos pais* ao lado da filha, Maria Rita. A campanha "VW Brasil 70: o novo veio de novo" (Volkswagen do Brasil, 2023) foi idealizada pela agência AlmapBBDO e divulgada em perfis de redes sociais, como *Instagram* e *Youtube*.

A representação 134/23 (Brasil. Conselho Nacional de Autorregulamentação Publicitária, 2023) foi aberta para avaliar dois pontos principais: a) se a utilização da imagem de Elis no anúncio foi respeitosa e ética; b) se haveria a necessidade de divulgação explícita da utilização de inteligência artificial na composição do anúncio.

O colegiado decidiu, por unanimidade e seguindo o parecer do relator, que não procedia a alegação de desrespeito à imagem da artista. Isso porque a utilização da imagem foi autorizada pelos herdeiros e retratava Elis em uma atividade que ela realizava em vida.

Com relação à especificação de que o conteúdo foi gerado por inteligência artificial, os conselheiros avaliaram várias recomendações de boas práticas sobre o tema, além de considerarem a falta de regulamentação específica vigente. Com base nisso, e seguindo a conselheira que emitiu o voto divergente, a maioria dos conselheiros (13 a 7) decidiu pelo arquivamento da denúncia. Eles enfatizaram que a transparência é um princípio ético essencial e, no caso em questão, consideraram que esse princípio foi respeitado, já que o uso da ferramenta era evidente na publicidade.

3.6.4.2 Brasil: Decisões dos TREs sobre deepfakes nas eleições 2024

O Laboratório de Governança e Regulação de Inteligência Artificial do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (LIA-IDP) e a ETHICS 4AI publicaram um relatório técnico "Construindo consensos: *deepfakes* nas eleições de 2024 – relatório das decisões dos TREs sobre *deepfakes*" (Junquilho; Silveira; Ferreira, 2024) acerca da interpretação dos tribunais eleitorais sobre o uso de *deepfakes* nas eleições brasileiras a partir da Resolução/TSE n. 23.732/2024, que alterou a Resolução/TSE n. 23.610/20219, dispondo sobre a propaganda eleitoral.

Foram identificadas um total de 57 decisões emitidas pelos Tribunais Regionais Eleitorais (TREs), das quais 56 puderam ser analisadas, já que uma estava sob segredo de justiça.

Ao analisar as decisões, a pesquisa identificou duas interpretações sobre a caracterização de um conteúdo como deepfake, nos termos do artigo 9º-C, § 1º, da Resolução TSE nº 23.610/2019:

1) O primeiro grupo inclui decisões que sustentam que o conteúdo deve aparentar ser autêntico, tornando-se quase impossível diferenciar o que é real daquilo que foi criado digitalmente. Nesse sentido, é a seguinte decisão

> Os *deepfakes*, que são uma tecnologia de Inteligência Artificial capaz de criar imagens, vídeos ou áudios extremamente realistas, são particularmente perigosos. Eles permitem que a voz ou a imagem de uma pessoa seja alterada para fazer parecer que ela disse ou fez algo que, na verdade, não fez. Isso representa um sério risco para o debate democrático, pois pode enganar os eleitores e influenciar suas decisões de forma enganosa e prejudicial ao processo eleitoral. O uso desse recurso tecnológico para criar falsamente a ideia de que o recorrido teria sido vaiado, em sessão da Assembleia Legislativa, restou comprovado nos autos pelo mero cotejamento entre os vídeos de ID29844901 e 29844902. Esse tipo de artifício é inadmissível, impondo-se reprimenda. (TRE-PE, 2024)

2) Já o segundo grupo inclui decisões que não consideram necessária a comprovação de alta verossimilhança. Nesse sentido, é a seguinte decisão:

> [...] a Resolução n. 23.610/2019 veda de forma cogente o uso de deep fake, tanto para prejudicar quanto para favorecer seja candidato ou na pré-campanha, vez que o que é proibido na campanha também é proibido na pré-campanha. [...] Assim, em que pese o vídeo ter sido destinado para as pessoas saberem do aniversário do avô de Gustavo e mesmo que ele não tenha trazido impactos ao pleito ou induzido o eleitor a erro, é certo que pelo uso de deep fake ele não poderia ser disponibilizado em rede social, mesmo havendo um destaque para informar que se cuidou de conteúdo criado por IA, haja vista a vedação ao uso de deep fakes tanto no período eleitoral quanto no período da pré-campanha. A proibição é total independentemente de in- duzir ou não o eleitorado a erro. (TRE-MG, 2024)

O relatório conclui:

> Assim, ao se analisar as decisões dos Tribunais Regionais Eleitorais, observou-se lacunas significativas, especialmente no que se refere à definição precisa e uniformizada dos conceitos de deep fake e desinformação, de modo que ausência de uma delimitação clara do que constitui deep fake, aliada à falta de um enquadramento adequado do fenômeno da desinformação, dificulta a análise jurídica eficaz desses casos.
>
> Sem critérios objetivos e conceitualmente sólidos, a jurisprudência acaba por tratar o tema de forma fragmentada, muitas vezes focando em aspectos técnicos, desassociados dos elementos contidos no art. 9o-C, da Res./TSE n. 23.610/2019, deixando de abordar o impacto sistêmico desse tipo de conteúdo no processo eleitoral. (Junquilho; Silveira; Ferreira, 2024)

3.6.5 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.6.5.1 Lei nº 15.123/2025

A introdução da Lei 15.123/2025 (Brasil, 2025) provocou uma mudança específica e relevante no contexto do emprego da inteligência artificial em relação às mulheres: um acréscimo de metade da pena para o delito de violência psicológica, conforme a atualização do parágrafo único do art. 147-B do Código Penal, o qual estabelece que "A pena é aumentada de metade se o crime é cometido mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima".

Verifica-se que o tipo penal aborda a criação de conteúdos como imagens, sons e montagens por meio de sistemas de inteligência artificial. Apesar da disposição legal expressa no "caput", que já contempla a inclusão do uso de tecnologia como um dos meios genéricos para causar danos à saúde psicológica da vítima, a justificativa para o aumento da penalidade destaca a intensificação da censurabilidade da conduta devido à capacidade de disseminação em larga escala, dificuldade de remoção e impacto emocional substancial, podendo resultar até em efeitos duradouros na imagem e vida social da vítima.

3.6.5.2 Resolução TSE nº 23.732/2024

O TSE (Tribunal Superior Eleitoral) tratou, por meio da Resolução nº 23.732/2024 (Brasil, 2024), do uso de inteligência artificial nas eleições ao modificar a Resolução nº 23.610/2019, que regulamenta a propaganda eleitoral:

> Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada.
>
> § 1º As informações mencionadas no caput deste artigo devem ser feitas em formato compatível com o tipo de veiculação e serem apresentadas:
>
> I – no início das peças ou da comunicação feitas por áudio;
>
> II – por rótulo (marca d'água) e na audiodescrição, nas peças que consistam em imagens estáticas;
>
> III – na forma dos incisos I e II desse parágrafo, nas peças ou comunicações feitas por vídeo ou áudio e vídeo;
>
> IV – em cada página ou face de material impresso em que utilizado o conteúdo produzido por inteligência artificial.
>
> §2º O disposto no caput e no §1º deste artigo não se aplica:
>
> I - aos ajustes destinados a melhorar a qualidade de imagem ou de som;
>
> II - à produção de elementos gráficos de identidade visual, vinhetas e logomarcas;
>
> III - a recursos de marketing de uso costumeiro em campanhas, como a montagem de imagens em que pessoas candidatas e apoiadoras aparentam figurar em registro fotográfico único utilizado na confecção de material impresso e digital de propaganda.
>
> § 3º O uso de chatbots, avatares e conteúdos sintéticos como artifício para intermediar a comunicação de campanha com pessoas naturais submete-se ao disposto no caput deste artigo, vedada qualquer simulação de interlocução com a pessoa candidata ou outra pessoa real.

§ 4º O descumprimento das regras previstas no caput e no § 3º deste artigo impõe a imediata remoção do conteúdo ou indisponibilidade do serviço de comunicação, por iniciativa do provedor de aplicação ou determinação judicial, sem prejuízo de apuração nos termos do § 2º do art. 9º-C desta Resolução.

"Art. 9º-C É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral.

§ 1º É proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia (deep fake).

§ 2º O descumprimento do previsto no caput e no § 1º deste artigo configura abuso do poder político e uso indevido dos meios de comunicação social, acarretando a cassação do registro ou do mandato, e impõe apuração das responsabilidades nos termos do § 1º do art. 323 do Código Eleitoral, sem prejuízo de aplicação de outras medidas cabíveis quanto à irregularidade da propaganda e à ilicitude do conteúdo.

A Resolução nº 23.732/2024 não proíbe o uso da inteligência artificial em casos de criação e modificação de conteúdos verdadeiros. Porém, o uso deve ser comunicado de forma clara e destacada por meio de uma rotulagem aos eleitores. Há proibição do uso de *deepfakes* (vídeos, fotos e áudios criados ou manipulados com inteligência artificial) com informações falsas ou enganosas sobre candidatos ou sobre o processo eleitoral. A referida resolução veda também o uso de robôs, por meio de *chatbots*, para imitar a voz de candidatos a fim de realizar conversas som eleitores ou com outras pessoas. Caso as regras sejam infringidas, o conteúdo deverá ser imediatamente retirado pelo próprio provedor de aplicação ou por determinação judicial.

3.6.5.3 Projeto de Lei nº 2.338/2022

O Projeto de Lei 2.338/2022, de autoria do senador Rodrigo Pacheco, que dispõe sobre o desenvolvimento, fomento e uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana, foi aprovado pelo plenário e encaminhado para a Câmara dos Deputados em 17/3/2025. A versão atual do projeto de lei regulamenta o uso da IA generativa, mas trata de forma genérica a temática do uso de imagem, áudio, voz e vídeo, como se verifica no art. 66:

> Art. 66. A utilização de conteúdos de imagem, áudio, voz ou vídeo que retratem ou identifiquem pessoas naturais pelos sistemas de IA deverá respeitar os direitos da personalidade, na forma prevista na Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), e na legislação pertinente.

3.6.5.4 Projeto de Lei nº 145/2024

O Projeto de Lei nº 145/2024, de autoria do senador Chico Rodrigues, altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para regular o uso de ferramentas de inteligência artificial para fins publicitários e coibir a publicidade enganosa com o uso dessas ferramentas.

> Art. 37- A. É proibida a publicação de mensagem publicitária em que a imagem ou voz de pessoa, viva ou falecida, seja manipulada mediante o emprego de sistemas de inteligência artificial para o processamento, análise e geração de imagens e áudio com o intuito de influenciar a percepção do consumidor quanto ao produto ou serviço e promover sua comercialização, salvo na hipótese de:
>
> I – consentimento prévio expresso do titular do direito de imagem, obtido de forma clara, inequívoca e documentada; e
>
> II – informação ao consumidor, de forma ostensiva, sempre que a imagem ou áudio for exibido, de que se trata de publicidade elaborada mediante uso de inteligência artificial.
>
> § 1o A publicação de mensagem publicitária em desacordo com o estabelecido no caput é considerada publicidade enganosa.
>
> § 2o Uma vez notificado da veiculação de publicidade enganosa, o veículo de comunicação social deverá interromper a divulgação, publicação ou transmissão da publicidade em até três dias úteis, independente de prévia comunicação ao anunciante, sob pena de responder solidariamente pela infração nos termos desta Lei, sem prejuízo das demais sanções civis, penais e administrativas cabíveis.
>
> § 3o A notificação de que trata o § 2o poderá ser judicial ou extrajudicial, sendo neste último caso realizada pelo titular dos direitos de imagem ou pelos órgãos federais, estaduais, do Distrito Federal e municipais com atribuições para fiscalizar e controlar o mercado de consumo.
>
> § 4o Para fins desta Lei considera-se veículo de comunicação qualquer meio de divulgação visual, auditiva ou audiovisual, incluindo rádio, televisão, sítios de internet e redes sociais. (Brasil, 2024)

3.6.5.5 Projeto de Lei nº 146/2024

O Projeto de Lei nº 146/2024, de autoria do senador Chico Rodrigues, altera o Código Penal (Decreto-lei 2.848, de 1940) para aumentar a pena nos crimes contra a honra cometidos em redes sociais que utilizem deepfake com inteligência artificial.

> Art. 141 [...]

§ 3o Se, na hipótese do § 2o deste artigo, houver a utilização de tecnologia de inteligência artificial para alterar a imagem de pessoa ou de som humano, com o objetivo de criar falso vídeo ou imagem, aplica-se em quíntuplo a pena.

§ 4o Nos termos do § 3o deste artigo, aplica-se em triplo a pena àquele que divulga falso vídeo ou imagem produzida por meio de inteligência artificial."

Art. 307 [...]

§ 1o Se na prática do crime houver a utilização de tecnologia de inteligência artificial para alterar a imagem de pessoa ou de som humano, com o objetivo de criar falso vídeo ou imagem, a pena será de reclusão, de um a cinco anos, e multa, se o fato não constitui elemento de crime mais grave.

§ 2o Incorre na pena prevista no § 1o deste artigo, reduzida de 1/3 até a metade, quem divulga falso vídeo ou imagem produzida por meio de inteligência artificial.

3.6.6 Comentários sobre o texto do projeto da reforma do Código Civil

No capítulo que trata da inteligência artificial, o Projeto de Lei nº 4, de 2025, traz diretrizes gerais que determinam que a criação de sistemas de inteligência artificial deve respeitar os direitos de personalidade, assegurando a implementação de tecnologias seguras e confiáveis para beneficiar indivíduos e empresas, bem como fomentar o progresso científico e tecnológico. Estabelece também que o avanço e a aplicação da inteligência artificial e da robótica em setores importantes para os direitos de personalidade devem ser supervisionados pela sociedade e orientados por legislação específica. Além disso, explicita que devem ser garantidos:

I – a não discriminação em relação às decisões, ao uso de dados e aos processos baseados em inteligência artificial;

II – condições de transparência, auditabilidade, explicabilidade, rastreabilidade, supervisão humana e governança;

III – a acessibilidade, a usabilidade e a confiabilidade;

IV – a atribuição de responsabilidade civil, pelo princípio da reparação integral dos danos, a uma pessoa natural ou jurídica em ambiente digital.

O Projeto de Lei nº 4, de 2025, prevê o direito à informação sobre a interação humana com sistemas de inteligência artificial, bem como o esclarecimento sobre o modelo geral de funcionamento e os critérios usados nas decisões automatizadas, em especial quando essas decisões impactam diretamente o acesso ou exercício de direitos, ou quando afetam de maneira significativa os interesses econômicos das pessoas.

Ao tratar das imagens criadas pela inteligência artificial, "o Código Civil passa a reconhecer que as imagens geradas por IA carregam efeitos, provocam emoções, influenciam decisões e precisam ser reguladas" (Porto, 2025a). Dessa forma, permite a utilização lícita da inteligência artificial para criar imagens de pessoas, sejam elas vivas ou falecidas, desde que sejam cumpridas as seguintes condições: a) obtenção prévia e expressa do consentimento informado da pessoa em questão, ou de seus herdeiros legais ou representantes, no caso de falecimento; b) manutenção do respeito à dignidade, à reputação, à presença e ao legado da pessoa representada digitalmente, evitando usos considerados difamatórios, desrespeitosos ou contrários ao seu modo de pensar ou ser. Isso deve estar de acordo com suas manifestações em vida, seja por meio de escritos, comportamentos ou qualquer outra forma de expressão cultural, religiosa ou política; c) para o uso comercial de criações relacionadas a uma pessoa falecida, é necessária autorização prévia e expressa do cônjuge, herdeiros, representantes ou uma disposição em testamento; d) cumprimento rigoroso de normas obrigatórias ou de ordem pública, especialmente as estabelecidas neste Código e na Constituição Federal.

É indispensável o consentimento explícito da pessoa viva ou, no caso de falecimento, dos herdeiros ou representantes legais, salvo disposições legais em contrário, para a produção de imagens de indivíduos com intuito de exploração comercial, sejam eles vivos ou falecidos. As imagens geradas estão sujeitas às regras de direitos autorais e à proteção de imagem, sendo que os herdeiros ou representantes legais da pessoa falecida têm a titularidade sobre esses direitos.

Como ressalta Laura Porto (2025a), a proposta visa preencher uma lacuna clara nas leis atuais, que envolve o uso não autorizado de imagens em ambientes digitais e automatizados, uma prática cada vez mais comum que afeta significativamente a privacidade e dignidade dos indivíduos. Essa questão é ainda mais relevante no caso de pessoas falecidas, pois diz respeito ao seu legado. O texto aborda essa questão de maneira direta, reconhecendo que a criação de imagens não é imparcial; ela pode servir como uma forma de homenagem, mas também ser usada para manipular, explorar ou difamar uma memória.

Importante ressaltar que não há impedimento para que a própria pessoa, enquanto viva, declare em testamento a rejeição ao uso da própria imagem por inteligência artificial após o falecimento. A declaração feita em testamento possui valor jurídico e deve ser respeitada tanto pelos herdeiros quanto por aqueles que eventualmente possuam os direitos de imagem.

Um aspecto essencial da proposta é a regulamentação do uso comercial das imagens que estabelece que qualquer utilização comercial de imagens geradas por inteligência artificial requer uma autorização específica. No caso de pessoas falecidas, essa permissão deve ser concedida pelos herdeiros, cônjuges ou prevista em um testamento.

Laura Porto (2025a) destaca que o ponto mais sensível e inovador dessa proposta está na exigência de respeito ao legado da pessoa natural, viva ou falecida, ou seja, a previsão normativa vai além da simples proteção da imagem no seu aspecto técnico para abarcar também os valores, as crenças, o modo de pensar e de existir. Nesse sentido, afirma que:

> Essa previsão é essencial porque reconhece algo que vai além da imagem, a memória tem valor jurídico, social e afetivo. A tecnologia não pode reescrever a história de uma pessoa para atender interesses de terceiros. Não se trata de impedir homenagens ou iniciativas legítimas, mas de garantir que elas não distorçam, forjem ou manipulem quem a pessoa foi. A dignidade, mesmo após a morte, continua sendo um direito, e o respeito à memória é parte desse reconhecimento. E ao proteger o legado, o Código Civil se atualiza para um tempo em que as pessoas poderão ter imagens recriadas por anos ou mesmo séculos.

O projeto prevê a obrigatoriedade da informação do uso de inteligência artificial na criação de qualquer imagem em respeito à transparência e garantindo a informação sobre a criação artificial[30].

3.7 Da celebração de contratos por meios digitais

O texto abaixo está contido no Capítulo VIII do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Da celebração de contratos por meios digitais".

> CAPÍTULO VIII - DA CELEBRAÇÃO DE CONTRATOS POR MEIOS DIGITAIS
>
> Art. 2027-AO. Entende-se por contrato digital todo acordo de vontades celebrado em ambiente digital, como os contratos eletrônicos, pactos via aplicativos, e-mail, ou qualquer outro meio tecnológico que permita a comunicação entre as partes e a criação de direitos e deveres entre elas, pela aceitação de proposta de negócio ou de oferta de produtos e serviços.

30 "Vale ressaltar que essa ideia surgiu quando nos deparamos com uma realidade cada vez mais comum nas redes sociais, influenciadores digitais criados por inteligência artificial com milhares de seguidores no Instagram, vendendo produtos, construindo rotinas perfeitas, exibindo corpos idealizados e padrões estéticos inatingíveis. Essas imagens, mesmo não sendo reais, impactam comportamentos, alimentam expectativas e influenciam, principalmente, adolescentes em fase de formação de identidade, mas esse é um assunto para outro artigo. Fato é que a ausência de identificação clara de que se trata de uma criação artificial aprofunda esse risco, pois leva o público a acreditar que está consumindo uma vida real, quando, na verdade, está interagindo com uma simulação. Não é apenas uma regra de forma, é uma medida de proteção contra manipulação emocional, desinformação e padrões inalcançáveis impostos silenciosamente por códigos de programação". (Porto, 2025a)

Art. 2027-AP. As mesmas regras que regem os contratos celebrados por instrumentos particulares ou públicos também se aplicam à regência da contratação feita em ambiente digital, atendidas suas especificidades e observado o tratamento previsto neste Código e na legislação especial.

Art. 2027-AQ. São princípios aplicáveis aos contratos celebrados por meios digitais:

I - imaterialidade: diante da formação e armazenamento por meio eletrônico;

II - autonomia privada: com o reconhecimento da liberdade das partes na criação de negócios digitais, desde que não contrariem a legislação vigente, sobretudo as normas cogentes e de ordem pública;

III - boa-fé: entendida como a exigência de que as partes atuem com honestidade, transparência, probidade, cooperação e lealdade durante a formação, a execução e a resolução dos contratos digitais;

IV - equivalência funcional: com o entendimento de que os contratos digitais possuem a mesma validade legal que os contratos tradicionais e analógicos, desde que cumpridos os requisitos legais para sua formação;

V - segurança jurídica: com a garantia de proteção aos direitos das partes envolvidas, assegurando a clareza, a precisão e a integridade dos termos acordados;

VI - função social do contrato: nos termos do que está assegurado nos arts. 421 e 2.035, parágrafo único, deste Código.

Art. 2027-AR. Na interpretação dos contratos digitais, devem ser considerados a sua funcionalidade conjunta, a compatibilidade, a interoperabilidade, a durabilidade e o seu uso comum e esperado.

Art. 2027-AS. O contrato formalizado por meio digital é considerado celebrado quando:

I - as partes manifestarem claramente a sua intenção de contratar, podendo a manifestação ser expressa por cliques, seleção de opções em interfaces digitais, assinaturas eletrônicas, ou por outros meios que demonstrem claramente a concordância com os termos propostos;

II - o objeto do contrato for lícito, possível, determinado ou determinável;

III – o contrato atender aos requisitos de forma e de solenidade previstos em lei, quando for o caso, incluindo a identificação das partes e a assinatura eletrônica, quando necessária.

Art. 2027-AT. Os contratos digitais, em regra, são considerados informais e não solenes, nos termos do art. 107 deste Código.

Art. 2027-AU. São considerados contratos inteligentes (smart contracts) aqueles nos quais alguma ou todas as obrigações contratuais são definidas ou executadas automaticamente por meio de um programa de computador, por meio da utilização de sequência de registros eletrônicos de dados e garantindo-se a integridade e a precisão de sua ordenação cronológica.

Parágrafo único. O fornecedor que utiliza contratos inteligentes ou, na sua ausência, a pessoa cujo comércio, negócio ou profissão envolva a sua implementação para terceiros, no contexto da execução de um acordo ou parte dele e ao disponibilizar dados, deve garantir que tais contratos cumpram os seguintes requisitos:

I – robustez e controle de acesso, para assegurar que o contrato inteligente foi projetado para oferecer mecanismos de controle de acesso e um grau muito elevado de segurança a fim de evitar erros funcionais e resistir à manipulação por terceiros;

II – término seguro e interrupção, para garantir que exista um mecanismo para encerrar a execução contínua de transações e que o contrato inteligente inclua funções internas capazes de reiniciar ou instruir o contrato a parar ou interromper a operação, especialmente para evitar futuras execuções acidentais;

III – auditabilidade, com arquivamento de dados e continuidade, para garantir, em circunstâncias em que um contrato inteligente precise ser encerrado ou desativado, a possibilidade de arquivar os seus dados transacionais, a sua lógica e o seu código a fim de manter-se o registro dos dados das operações passadas;

IV – controle de acesso, para assegurar que o contrato inteligente esteja protegido por meio de mecanismos rigorosos de controle de acesso nas camadas de governança; e

V – consistência, para garantir a conformidade com os termos do acordo que o contrato inteligente executa.

Art. 2027-AV. O contrato celebrado por aplicativo digital é válido e eficaz, se atendidos os requisitos legais previstos neste Código.

Parágrafo único. Para fins deste artigo, entende-se por aplicativo digital qualquer plataforma, software ou sistema eletrônico que

> permita a celebração, gestão e execução de contratos que tenham por objeto a intermediação do uso, gozo e fruição de coisa não fungível ou imaterial.

3.7.1 Abordagem teórica da temática

Diante da crescente importância das plataformas tecnológicas e da relevância dos contratos digitais nas transações realizadas cotidianamente, tornou-se essencial a regulamentação dos contratos digitais para garantia da sua validade e da sua eficácia. Em linhas gerais, pode-se dizer que os contratos digitais são aqueles cuja manifestação de vontade das partes se dá por meio eletrônico ou, ainda, cuja celebração se expressa por meio eletrônico. Nos termos do Art. 2027-AO do Projeto de Lei no. 4, de 2025:

> Entende-se por contrato digital todo acordo de vontades celebrado em ambiente digital, como os contratos eletrônicos, pactos via aplicativos, e-mail, ou qualquer outro meio tecnológico que permita a comunicação entre as partes e a criação de direitos e deveres entre elas, pela aceitação de proposta de negócio ou de oferta de produtos e serviços.

A depuração dos contornos atuais dos contratos digitais passa, antes, pela compreensão dos pressupostos teóricos. Tais pressupostos são costumeiramente tratados pela literatura civilista ao tratar da Teoria Geral dos Atos Jurídicos – em especial, dos negócios jurídicos – e da Teoria Geral dos Contratos.

Os contratos são negócios jurídicos, derivados de manifestações de vontade tendentes à criação, à modificação ou à extinção de uma relação jurídica. Há, neles, um complexo de direitos e obrigações com escopo eminentemente patrimonial (Azevedo, 2019, p. 28). Com efeito, o contrato, de forma amplamente aceita, pode ser definido como um acordo de vontades entre duas ou mais partes, com o propósito de adquirir, preservar, modificar ou extinguir direitos.

As declarações de vontade e a exteriorização conjugam-se a fim de perseguir interesses de ambas as partes. Trata-se, nada mais, do que o denominado princípio do consensualismo, sendo suficiente o acerto de vontades para a deflagração do nexo contratual.

Por sua vez, o contrato digital pode ser entendido como uma modalidade de formalização contratual que sucede os mesmos requisitos de validade aplicáveis aos contratos tradicionais, abrangendo os mesmos tipos de objetos. A principal diferença reside no meio ou instrumento – leia-se, forma – utilizado para a concretização dele.

Os contratos digitais, portanto, são aqueles cuja manifestação de vontade das partes se dá em ambiente digital ou qualquer outro meio tecnológico que permita a comunicação entre as partes e a criação de direitos e deveres entre elas. O ambiente digital ou outro meio tecnológico é mera técnica diversa para o encontro das vontades, que encampa uma nova modalidade de formação contratual.

Nada obstante sejam utilizados frequentemente como sinônimos, parte da literatura distingue contratos eletrônicos, contratos digitais e contratos virtuais. Nessa esteira, releva a preleção de Júlio Canello (2007), que afirma:

> O contrato digital pode ser entendido como aquele formado e "materializado" digitalmente, ou seja, através de linguagem própria de computadores (que pode ser reduzida à lógica binária). É digital o contrato que se manifesta por ser uma sequência de bits organizada de forma que seja codificada e decodificada por um computador e tornar-se manifestável como contrato. Portanto, o que o qualifica enquanto tal é o processo de digitalização das informações, podendo estar lotado em qualquer suporte físico de memória. Já o contrato virtual é aquele que, além de ser digital, forma-se através do uso, em geral, da Internet. Não basta que esteja na forma digital (sequência de bits), importa, também, que sofra um processo de virtualização, que, mesmo não estando lotado na memória do computador de ambas as partes contratantes, seja passível de atualização e acesso através de uma rede de computadores. Aqui, o que o diferencia da forma digital é que o contrato pode, através dos métodos adequados, se acessado em qualquer terminar da rede. Assim, num sentido alargado, o contrato eletrônico é aquele que faz uso de um instrumento ou técnica eletrônica para sua formação, manifestação de vontade e, às vezes, "materialização", podendo ser, também, digital e virtual.

Já os contratos inteligentes, também previstos no Projeto de Lei no. 4, de 2025, conhecidos pelo termo em inglês *smart contracts*, foram concebidos por Nick Szabo, em trabalho publicado em 1994. Trata-se de um protocolo de transação computadorizado que executa os termos de um contrato, reduzindo os custos e os riscos de descumprimento, seja acidental ou proposital, além de diminuir a necessidade de intermediários, como bancos, advogados, contadores e corretores (Szabo, 1994). Segundo Cintia Rosa Pereira de Lima e Walter Francisco Sampaio Neto (2024):

> O que difere os smart contracts dos demais contratos eletrônicos, não é sua autoexecutoriedade, que pode ser programada em outras formas eletrônicas de contrato, mas na natureza descentralizada do vínculo que se pretende estabelecer entre as partes. É desse aspecto que decorre a autoexecutoriedade do smart contract porque não existindo intermediários nas redes, os programas (smart contracts) com seus códigos inseridos na rede, rodarão de forma automatizada.

Quanto à formação dos contratos digitais, deve-se rememorar que, no escopo dos contratos regulados pelo Código Civil atual, a proposta é elemento necessário para a veiculação da manifestação de vontade. Como resultado do encontro das vontades, a formação do contrato pressupõe a exteriorização dessas. A iniciativa para originar o diálogo contratual é denominada de proposta ou policitação. Será considerada como

proposta se a provocação contiver todos os elementos essenciais do contrato, sendo precisa e completa. Deve haver, ainda, manifestação de expressa intenção de contratar (Bioni; Lisboa, 2010).

No caso de contratos entre ausentes, a literatura encampa duas teorias explicativas a respeito da formação de contratos. Segundo o escorço da Teoria da Cognição, o contrato entre ausentes somente se considera formado quando a resposta do aceitante chegasse ao conhecimento do proponente. Já conforme a Teoria da Agnição, dispensa-se que a resposta chegue ao conhecimento do proponente. A subteoria acolhida pelo Código Civil foi a denominada Subteoria da Expedição, conquanto considere-se formado o contrato no momento de expedição da resposta. O cotejo dos dispositivos transparece a impressão de que foi adotada a vertente teórica da expedição:

> Art. 434. Os contratos entre ausentes tornam-se perfeitos desde que a aceitação é expedida, exceto:
>
> I — no caso do artigo antecedente;
>
> II — se o proponente se houver comprometido a esperar resposta;
>
> III — se ela não chegar no prazo convencionado.

A formulação da proposta pode ser precedida por uma fase preliminar, dada a complexidade das relações contratuais. Essa etapa inicial envolve discussões sobre o conteúdo das obrigações, permitindo que a proposta final de contratação reúna todos os elementos essenciais do acordo. É justamente por conta desses elementos que distinguem a proposta das tratativas preliminares que surge o efeito vinculante na primeira, funcionando como o verdadeiro "divisor de águas" em relação à segunda.

Assim, a proposta, por si só, não constitui o negócio jurídico mencionado, sendo definida como uma declaração de vontade receptícia. É nesse contexto que surge a aceitação, representando a resposta do policitado, determinando, por fim, a celebração ou não do contrato (Bioni; Lisboa, 2010). A aceitação, tal como a proposta, poderá se efetivar por meio da linguagem eletrônica ou por meio digital, hipótese na qual se caracterizará a aceitação eletrônica.

No comércio eletrônico, a parte pode manifestar a aceitação por meio de simples ações, como tocar em símbolos ou ícones e realizar cliques. Da mesma forma, o início da execução do contrato, como em uma compra e venda, ocorre quando o comprador efetua o pagamento, inserindo os dados do cartão de crédito na página eletrônica, ou clica em botões como "concordo" ou "aceito", exteriorizando a concordância com a oferta.

Nesses casos, não há uma declaração formal de vontade dirigida ao ofertante; em vez disso, comportamentos como usufruir do bem ou serviço, como nos downloads de programas de computador, são considerados atos conclusivos, que demonstram a aceitação da proposta. Assim, a concordância expressa-se por meio dessas ações, estabelecendo o vínculo contratual.

Sob tal perspectiva, a literatura manifesta o consentimento de diversas formas: i) de forma intersistêmica, por meio de sistemas pré-programados, pelos quais as partes utilizam-se do computador apenas como um ponto convergente de vontades preexistentes; ii) de forma interpessoal, como um meio para que as partes interajam e acabem por formar o consentimento contratual (como chats e chamadas de vídeo), e; iii) de forma interativa, quando deriva de uma interação entre uma pessoa e um sistema aplicativo previamente programado (Bioni; Lisboa, 2010).

3.7.2 Experiências normativas do direito estrangeiro e transnacional

3.7.2.1 União Europeia

No contexto europeu, observa-se um movimento regulatório voltado a conferir maior estabilidade normativa e previsibilidade jurídica ao emprego de tecnologias como a blockchain e os contratos inteligentes. Dentre tais iniciativas, destaca-se a publicação, por parte do European Law Institute (ELI) (União Europeia, 2022) de um conjunto de princípios orientadores que, ao mesmo tempo em que propõem diretrizes para interpretação e aplicação desses contratos no quadro normativo atual, buscam assegurar a proteção do consumidor e promover a integração segura dessas novas modalidades contratuais aos sistemas jurídicos vigentes.

Paralelamente a esse esforço, a União Europeia editou o EU Data Act (União Europeia, 2023), regulamento que, ao mesmo tempo em que consolida um marco para o compartilhamento e a reutilização de dados entre diferentes setores da economia, avança na direção de reconhecer expressamente a importância jurídica dos contratos inteligentes dentro desse novo ecossistema digital, conferindo-lhes caráter vinculativo e assegurando que sejam tratados como instrumentos plenamente válidos e eficazes nas relações comerciais.

O art. 36 do referido Regulamento traz disposições que guardam semelhança com as previstas na legislação brasileira para os contratos inteligentes, prevendo, por exemplo, que tais contratos devem ser concebidos de forma a incorporar mecanismos técnicos robustos voltados ao controle de acesso e à segurança, com a finalidade de prevenir falhas operacionais e garantir resistência a eventuais tentativas de manipulação externa. Ainda, o dispositivo determina a obrigatoriedade de implementação de funcionalidades que permitam a interrupção da execução contínua das transações, incluindo a possibilidade de reinicialização ou paralisação segura do contrato, de modo a evitar que ocorram execuções não intencionais ou acidentais.

Outro aspecto relevante, também previsto no art. 36, é a necessidade de assegurar, nos casos de rescisão ou desativação do contrato inteligente, a existência de procedimentos que viabilizem o arquivamento das informações referentes às transações realizadas,

bem como da lógica de programação e do próprio código do contrato, com o objetivo de preservar a auditabilidade e o rastreamento das operações. Ademais, o dispositivo reforça a exigência de que os contratos inteligentes estejam devidamente protegidos por controles de acesso rigorosos, que são aplicáveis tanto aos procedimentos de governança quanto à operacionalização dos contratos em si; considera-se igualmente essencial que sua execução observe estrita conformidade com os termos previamente acordados no contrato de compartilhamento de dados que lhes serve de base, assegurando, assim, o cumprimento das obrigações estabelecidas entre as partes contratantes.

3.7.2.2 Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL)

A denominada Convenção de Comunicações Eletrônicas (ONU, 2005), formalmente conhecida como Convenção das Nações Unidas sobre o Uso de Comunicações Eletrônicas em Contratos Internacionais, foi adotada em 2005 e tem, como finalidade central, ainda que de forma não exclusiva, a criação de um conjunto de parâmetros normativos destinados a reger o uso de tecnologias eletrônicas no âmbito da formação de contratos internacionais. O seu principal objetivo é assegurar que tais contratos, celebrados por meios digitais, venham a ter o mesmo reconhecimento jurídico que tradicionalmente se conferia aos instrumentos firmados em suporte físico, superando, assim, obstáculos de ordem formal que, de outro modo, poderiam comprometer sua validade ou mesmo sua eficácia perante os sistemas jurídicos nacionais.

A Convenção, ao abordar as etapas da formação contratual, dedica atenção tanto à constituição do vínculo jurídico entre os contratantes quanto à definição precisa do momento de envio e recebimento das comunicações eletrônicas, além de reforçar a obrigatoriedade de se reconhecer a força vinculante dessas manifestações de vontade expressas por via eletrônica. No seu art. 1º, inciso I, é delimitado o escopo de aplicação da Convenção, que se dirige especificamente a comunicações eletrônicas vinculadas à formação ou execução de contratos envolvendo partes estabelecidas em diferentes Estados, o que não exclui, contudo, a possibilidade de aplicação subsidiária de suas regras a outras situações análogas.

Além dessas previsões, a Convenção de Comunicações Eletrônicas contempla um conjunto de definições para a correta interpretação de seu conteúdo normativo: o conceito de "comunicação eletrônica", nos termos do artigo 4(b), compreende qualquer comunicação realizada entre as partes por meio de mensagens de dados. A expressão "mensagem de dados", por sua vez, conforme disciplinado no artigo 4(c), abrange toda e qualquer informação que tenha sido gerada, transmitida, recebida ou armazenada por meios eletrônicos, ópticos ou similares, incluindo formatos tão variados quanto intercâmbio eletrônico de dados (EDI), correio eletrônico, telegrama, telex ou mesmo fax.

Todavia, até o momento, nenhuma das regulamentações mencionadas definiu o que são "contratos digitais" de forma tão específica como a proposta brasileira. Isso é consi-

derado um passo muito importante no cenário brasileiro, pois não apenas regulamenta mensagens de dados e comunicações eletrônicas, mas vai além, ao pressupor que, se as partes acordaram em um contrato de forma digital, a regulamentação deve se aplicar e regular os passos subsequentes à formação do contrato. A celebração de um contrato em forma digital é considerada possível, e o regulamento trata de aspectos essenciais para as partes após a formação do contrato. O artigo não se limita a abordar a comunicação eletrônica, mas sim o cenário contratual digital como um todo.

Além dessa normativa, a UNCITRAL introduziu, em 1996, a Lei Modelo da UNCITRAL sobre Comércio Eletrônico adotada por mais de 80 estados e cerca de 170 jurisdições. Essa lei modelo oferece um quadro legal para contratos eletrônicos, assinaturas eletrônicas e outras transações digitais. O objetivo é eliminar barreiras ao uso de contratos eletrônicos, garantindo que sejam tão válidos e executáveis quanto os contratos tradicionais em papel. A Lei Modelo da UNCITRAL sobre Comércio Eletrônico foi o primeiro texto legislativo a adotar os princípios fundamentais da não discriminação, neutralidade tecnológica e equivalência funcional, amplamente reconhecidos como os pilares do direito moderno do comércio eletrônico.

O princípio da não discriminação garante que um documento não seja negado por efeito legal, validade ou executabilidade apenas por estar em formato eletrônico. A neutralidade tecnológica exige que as disposições sejam neutras em relação à tecnologia utilizada para que possam se adaptar a futuros desenvolvimentos sem a necessidade de novas regulamentações. A equivalência funcional estabelece critérios sob os quais as comunicações eletrônicas podem ser consideradas equivalentes às comunicações em papel. O Art. 2a da Lei Modelo define "mensagem de dados" como informações geradas, enviadas, recebidas ou armazenadas por meios eletrônicos, ópticos ou similares, incluindo intercâmbio eletrônico de dados, correio eletrônico, telegrama, telex ou telecópia. O Art. 2b define o "Intercâmbio Eletrônico de Dados" como a transferência eletrônica de informações de um computador para outro, utilizando um padrão acordado para estruturar as informações.

3.7.2.3 Alemanha

Atualmente, o Código Civil alemão prevê que contratos podem ser celebrados de forma verbal, por escrito com assinatura ou assinatura eletrônica qualificada. Com a entrada em vigor da Diretiva Europeia sobre a Venda de Bens em 1º de janeiro de 2022, o Código Civil Alemão (BGB) passou a incorporar os §§ 327 e seguintes, que disciplinam aspectos relacionados a "conteúdos digitais" e "serviços digitais". Tais categorias encontram definição no § 327, inciso II. O termo "conteúdos digitais" abrange dados que sejam gerados e disponibilizados em meio digital. Já os "serviços digitais" correspondem a prestações que viabilizam ao consumidor: (i) a criação, o processamento, o armazenamento ou o acesso a dados digitais; ou (ii) o compartilhamento de dados produzidos

ou carregados digitalmente pelo próprio consumidor ou por terceiros, além da interação com tais dados. Entre os principais exemplos de conteúdos digitais, destacam-se softwares, arquivos de áudio e vídeo, músicas, jogos eletrônicos, livros digitais (e-books), aplicativos para dispositivos móveis e outras formas de publicação em formato eletrônico. No entanto, essa regulamentação não trata da celebração de contratos digitais, mas sim da prestação de conteúdos digitais.

Sobre o conceito de equivalência funcional entre contratos tradicionais (celebrados por instrumentos particulares ou públicos) e contratos digitais, assim como no Brasil[31], as leis alemãs também estabelecem requisitos específicos de forma para alguns contratos, como compra e venda, cancelamento de contrato trabalhista, contratos de aluguel, entre outros. Além disso, na Alemanha, já existem cartórios com registros digitais, e com o avanço de tecnologias como *blockchain*, pode se tornar possível que autenticações notariais também ocorram de forma digital. Nesse sentido, o artigo abre espaço para desenvolvimentos futuros.

O § 126a do Código Civil Alemão (BGB) estabelece que contratos podem ser celebrados por meios eletrônicos, equiparando-os, em termos de validade, aos contratos físicos. Na Alemanha, não há obrigação de que os contratos sejam físicos, a menos que a lei exija uma forma específica. O princípio da *äquivalente Funktionalität* (equivalência funcional) é amplamente aceito no direito alemão. A legislação como o *Signaturgesetz* (Lei de Assinaturas Eletrônicas), garante que contratos eletrônicos sejam considerados equivalentes aos contratos físicos, desde que atendam aos requisitos formais, como o uso de assinaturas eletrônicas qualificadas.

O BGB foca mais nos aspectos tradicionais de oferta e aceitação, sem abordar diretamente questões tecnológicas. No entanto, o princípio da equivalência funcional é amplamente aceito, e os contratos digitais podem ter o mesmo efeito dos contratos físicos ou verbais, o que, de maneira tangencial, se relaciona à ideia de funcionalidade e compatibilidade técnica.

O § 126 BGB trata da *Schriftform* (forma escrita), que pode ser substituída por uma assinatura eletrônica qualificada conforme o *Signaturgesetz* (Lei de Assinaturas Eletrônicas), implementada de acordo com as diretrizes da União Europeia. Portanto, uma assinatura eletrônica pode substituir a assinatura física, desde que cumpra os requisitos legais de autenticidade e segurança.

No direito alemão, os contratos inteligentes ainda não possuem uma regulamentação específica consolidada, mas são discutidos à luz dos princípios já estabelecidos. A abordagem legal é mais conservadora, baseada nos princípios tradicionais dos contratos.

31 "Art. 2.027-AP. As mesmas regras que regem os contratos celebrados por instrumentos particulares ou públicos também se aplicam à regência da contratação feita em ambiente digital, atendidas suas especificidades e observado o tratamento previsto neste Código e na legislação especial."

O direito alemão exige que os contratos sigam certos requisitos de clareza de vontade e capacidade de cumprimento. A execução automática de obrigações contratuais, como nos contratos inteligentes, não contraria os princípios do direito alemão, desde que as partes compreendam e aceitem os termos. No entanto, o BGB ainda não aborda explicitamente a execução automática.

3.7.2.4 Estados Unidos

Atualmente, não há uma lei federal nos EUA que defina explicitamente os contratos inteligentes, mas leis como o E-Sign Act Electronic Signatures in Global and National Commerce Act (2000) fornecem uma base para a aplicabilidade jurídica deles. Além disso, alguns estados, como o Arizona, promulgaram leis que reconhecem expressamente os contratos inteligentes. No Arizona, os contratos inteligentes são regulamentados pelo Estatuto Revisado do Arizona § 44-7061 (2024), parte de uma legislação mais ampla sobre transações eletrônicas e tecnologia blockchain. Esse estatuto define contratos inteligentes como programas baseados em plataformas que operam de forma descentralizada. Especificamente, ele estabelece que:

1. Reconhecimento legal: os contratos inteligentes têm validade jurídica que não pode ser negada apenas por incorporarem termos de forma digital;

2. Definição de *blockchain*: a lei define a tecnologia blockchain, que pode ser usada de forma pública ou privada, destacando a segurança criptográfica e imutabilidade dela;

3. Direitos de propriedade: indivíduos que usam a tecnologia blockchain para proteger as próprias informações mantêm os direitos de propriedade, que continuam mesmo após a informação ser assegurada via blockchain.

Essas normas guardam plena conformidade com o *Arizona Electronic Transactions Act* (AETA), que garante a validade e a eficácia jurídica de assinaturas e registros digitais, abrangendo expressamente aqueles decorrentes da execução de contratos inteligentes.

De forma semelhante, o estado do Tennessee, por meio de legislação sancionada em março de 2018, passou a reconhecer oficialmente a força jurídica tanto da tecnologia blockchain quanto dos contratos inteligentes aplicados a transações eletrônicas, definindo-os como programas acionados por eventos e executados de maneira descentralizada. No mesmo sentido, o estado de Nevada (2017), ao incluir os contratos inteligentes no Capítulo 719 dos Estatutos Revisados de Nevada (NRS), mais especificamente no NRS 719.240, estabeleceu de forma inequívoca que esses instrumentos possuem caráter vinculante e que sua eficácia legal não pode ser negada pelo simples fato de se apresentarem em formato eletrônico ou de operarem por meio de tecnologia blockchain.

3.7.2.5 Reino Unido

No Reino Unido, os contratos inteligentes são regidos principalmente pelos princípios de *Common law*, em vez de regulamentos estatutários específicos. A *UK Jurisdiction Task-force* (UKJT) emitiu uma declaração legal afirmando que contratos inteligentes podem ser considerados juridicamente vinculativos sob a lei inglesa, desde que os requisitos fundamentais para a formação de um contrato sejam atendidos.

3.7.2.6 Síntese analítica das experiências normativas de direito estrangeiro e transnacional

O estudo das experiências normativas estrangeiras e transnacionais permitiu verificar uma tendência no reconhecimento da validade jurídica dos contratos digitais e dos contratos inteligentes, ainda que o detalhamento normativo varie entre as experiências normativas estudadas.

Na Alemanha, o reconhecimento jurídico dos contratos digitais decorre dos princípios gerais do Código Civil (BGB) e das normas europeias (eIDAS), baseando-se em autonomia privada, boa-fé e equivalência funcional, mas ainda sem disciplina técnica específica para contratos inteligentes. Nos EUA, prevalece a legislação estadual (como Arizona e Nevada), que reconhece a validade jurídica dos contratos inteligentes e do uso de blockchain, com forte ênfase na neutralidade tecnológica, mas sem o nível de detalhamento técnico do PL 4/2025.

Na União Europeia, o *EU Data Act* e os princípios do *European Law Institute* começam a incorporar requisitos técnicos similares ao projeto brasileiro, sobretudo em termos de segurança, término seguro e auditabilidade dos contratos inteligentes. O Reino Unido e as normas da UNCITRAL também reconhecem contratos digitais e inteligentes, mas, em geral, ainda com foco em princípios contratuais tradicionais e na neutralidade tecnológica, sem o detalhamento normativo apresentado pelo Projeto de Lei nº 4, de 2025.

3.7.3 Estudos de caso

3.7.3.1 Estados Unidos

Os EUA são um dos países com o maior volume de litígios relacionados a contratos inteligentes. No caso CFTC v. *My Big Coin Pay*, Inc. (2018), a Comissão de Comércio CFTC lidou com um caso envolvendo um contrato inteligente relacionado ao uso fraudulento de criptomoedas. Embora o foco estivesse na fraude, a tecnologia blockchain e os contratos inteligentes fizeram parte do cenário do caso. A CFTC apresentou uma queixa contra a *My Big Coin Pay*, Inc., alegando que a empresa estava envolvida em fraudes relacionadas à sua criptomoeda, "My Big Coin". A My Big Coin afirmava ser uma moeda digital respaldada por ouro e outros ativos, atraindo investidores em busca

de oportunidades no crescente mercado de criptomoedas. No entanto, a CFTC acusou a empresa e o fundador dela de enganar os investidores ao falsear o valor e respaldo da criptomoeda. Especificamente, a queixa descreveu que os réus se apropriaram de fundos de investidores para uso pessoal, em vez de utilizá-los conforme prometido para desenvolver a moeda e plataforma associada.

Embora o caso em análise não tenha o foco em contratos inteligentes, destacam-se vários pontos relevantes sobre as suas potenciais implicações. Embora os contratos inteligentes representem um avanço relevante na ampliação da previsibilidade, da rastreabilidade e da transparência nas transações comerciais – funcionando como um possível fator de contenção de condutas fraudulentas, em razão de sua estrutura baseada na execução automática de obrigações e na manutenção de registros permanentes das operações realizadas –, tais instrumentos não são suficientes, por si só, para eliminar o risco de manipulações ou outras práticas ilícitas, o que revela limitações importantes em sua eficácia preventiva. A isso se soma o fato de que o episódio analisado trouxe à tona deficiências estruturais no marco regulatório vigente, demonstrando as dificuldades enfrentadas pelos órgãos de fiscalização.

No geral, o caso CFTC v. *My Big Coin* é fundamental para entender a interseção entre criptomoedas, contratos inteligentes e estruturas regulatórias, enfatizando a necessidade de definições e proteções legais robustas no cenário digital em evolução.

3.7.3.2 Reino Unido

O Reino Unido ainda não apresenta muitos casos amplamente divulgados, mas os tribunais britânicos já começaram a enfrentar questões relacionadas a *blockchain* e aos contratos inteligentes. Em 2019, um relatório elaborado pelo UK Jurisdiction Taskforce (UKJT) apontou que os contratos inteligentes, dentro do contexto da legislação inglesa, poderiam ser considerados aplicáveis e suscetíveis de execução judicial, o que, de certa forma, contribuiria para facilitar a resolução de eventuais litígios futuros envolvendo tais instrumentos.

Um exemplo recente foi o caso relacionado a *AA v. Persons Unknown*, de 2019, no qual o tribunal inglês lidou com o uso de criptomoedas baseadas em *blockchain* que estavam associadas a contratos inteligentes. Neste caso, houve subtração ilícita de ativos digitais, representados por criptomoedas, que foram desviadas para contas não identificáveis. Com o intuito de rastrear e recuperar os valores subtraídos, a parte autora pleiteou judicialmente a adoção de medidas cautelares, incluindo ordens para impedir novas movimentações dos ativos desviados. Embora a controvérsia central girasse em torno de um crime, o caso acabou por evidenciar, ainda que de forma não direta, o papel dos contratos inteligentes como um fator potencial de reforço à segurança das transações digitais, na medida em que, por operarem sobre a base da tecnologia blockchain e por

estabelecerem termos contratuais imutáveis sem o prévio consenso das partes envolvidas, tais instrumentos oferecem um ambiente que tende a privilegiar a transparência e a reduzir, ao menos em tese, a ocorrência de fraudes semelhantes àquela sofrida por AA.

3.7.3.3 Singapura

Singapura também já presenciou disputas envolvendo contratos inteligentes e blockchain (Orionw Law, 2020). Um caso importante é o B2C2 Ltd. v. Quoine Pte Ltd (2019) em que a B2C2, uma empresa de criptomoedas, utilizou um contrato inteligente para realizar transações de câmbio na *exchange* da Quoine. Devido a uma falha de natureza técnica na plataforma, os contratos inteligentes acabaram por desencadear uma sequência de transações que, em termos financeiros, resultaram em prejuízos consideráveis para a Quoine, o que motivou a empresa a buscar, em momento posterior, formas de reverter os efeitos dessas operações. Contudo, ao apreciar o litígio, o Tribunal de Singapura entendeu que as transações efetuadas por meio desses mecanismos automatizados deveriam ser tratadas como juridicamente vinculantes, fixando, com isso, um precedente de relevo para discussões futuras que envolvam instrumentos digitais semelhantes. Além de esclarecer, com maior profundidade, a forma como a doutrina do erro deve ser aplicada no contexto de contratos digitais, a decisão reafirmou a tese de que a mera ocorrência de um erro técnico não constitui, por si só, fundamento suficiente para a invalidação de um contrato, sobretudo quando se verifica que ambas as partes tinham compreensão e concordância quanto aos termos estabelecidos no momento da celebração do acordo.

Esse entendimento reforça a necessidade de que os agentes envolvidos em transações com criptomoedas adotem procedimentos de diligência ainda mais rigorosos, tendo em vista que a automação da execução contratual – elemento característico dos contratos inteligentes – não apenas elimina a presença de intermediários, como também amplia a segurança e a confiança nas transações realizadas. Desse modo, o caso B2C2 Ltd. v. Quoine Pte Ltd. consolida a exigibilidade dos contratos digitais, mas também demonstra a confiança na blockchain seja comercialmente resistente.

3.7.4 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.7.4.1 Projeto de Lei nº 954/2022

O Projeto de Lei nº. 954/2022 foi apresentado em 19 de abril de 2022 pelo deputado Luizão Goulart, e tem por objetivo alterar a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), "para dispor sobre contratos estruturados sob definições para sua execução, no todo ou em parte, de modo automatizado e mediante emprego de plataformas eletrônicas e soluções tecnológicas que assegurem autonomia, descentralização e autossuficiência, dispensando intermediários para a implementação do acordo entre os contratantes ou garantir a autenticidade".

O projeto é sucinto, trazendo duas disposições principais:

> Art. 1º O art. 425 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), passa a vigorar com as seguintes alterações:
>
> Art. 425. .....
>
> Parágrafo único. O disposto no caput aplica-se inclusive a contratos estruturados sob definições para sua execução, no todo ou em parte, de modo automatizado e mediante emprego de plataformas eletrônicas e soluções tecnológicas que assegurem autonomia, descentralização e autossuficiência, dispensando intermediários para a implementação do acordo entre os contratantes ou garantir a autenticidade. (NR)"
>
> Art. 2º A Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), passa a vigorar acrescida do seguinte art. 425-A:
>
> "Art. 425-A. Em caso de controvérsia ou litígio envolvendo a execução de contratos referidos no parágrafo único do caput do art. 425 desta Lei, a aplicação do direito dar-se-á mediante ponderação e balanceamento dos princípios e normas aplicáveis vigentes, buscando-se preservar:
>
> I – boas práticas de governança e abordagem baseada em riscos; e
>
> II – a solidez, eficiência e confiabilidade dos contratos e atos relativos à respectiva execução.

3.7.5 Comentários sobre o texto do projeto da reforma do Código Civil

O Projeto de Lei nº 4, de 2025, traz uma definição ampla de "contrato digital", adaptando-se à realidade tecnológica e ao crescente uso de plataformas digitais nas relações contratuais . Como já visto anteriormente, o conceito de "contrato digital" é apresentado como um "acordo de vontades celebrado em ambiente digital", abrangendo os contratos eletrônicos e pactos realizados por diversos meios tecnológicos, como aplicativos e e-mails. A definição não limita os tipos de tecnologia e a inclusão de "qualquer outro meio tecnológico que permita a comunicação entre as partes" traz flexibilidade para que outras ferramentas digitais possam ser incluídas. Isso assegura que o ponto central da normatização é a manifestação da vontade das partes.

Reconhece que as comunicações eletrônicas são formas válidas de expressar consentimento, e a aceitação de uma proposta pode ocorrer digitalmente, desde que esteja clara a intenção de vincular-se às obrigações contratuais.

Nesse sentido, o texto proposto[32] abrange o conceito da "equivalência funcional" entre os contratos tradicionais (celebrados por instrumentos particulares ou públicos) e os

32 "Art. 2.027-AP. As mesmas regras que regem os contratos celebrados por instrumentos particulares ou públicos também se aplicam à regência da contratação feita em ambiente digital, atendidas suas especificidades e observado o tratamento previsto neste Código e na legislação especial."

contratos digitais. Esse princípio estabelece que a função jurídica de um contrato não depende da forma (meio físico ou digital), mas sim da capacidade de expressar a vontade das partes de maneira clara e verificável. O artigo reforça que, independentemente da contratação ocorrer em um meio digital, os mesmos princípios e as mesmas regras que regem os contratos tradicionais se aplicam para os celebrados em meio digital. A equiparação entre contratos tradicionais e digitais assegura a validade e eficácia jurídicas, independentemente do meio utilizado.

Embora o artigo preveja a aplicação das mesmas regras que regem os contratos tradicionais, ressalta a importância de atender às especificidades do ambiente digital. Isso implica que, apesar de o contrato digital estar sujeito às mesmas normas gerais, existem peculiaridades próprias desse meio que devem ser consideradas, como a autenticação e validade das assinaturas, a segurança e a integridade do contrato, a prova do consentimento, previstas em normas específicas, tais como Lei de Assinaturas Eletrônicas (Lei 14.063/2020), o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD).

O texto do projeto de lei estabelece os seguintes princípios fundamentais para a regulação dos contratos celebrados por meios digitais, refletindo as características específicas desse ambiente e garantindo a adaptação das normas contratuais tradicionais ao contexto digital:

> I – imaterialidade: diante da formação e armazenamento por meio eletrônico;
>
> II – autonomia privada: com o reconhecimento da liberdade das partes na criação de negócios digitais, desde que não contrariem a legislação vigente, sobretudo as normas cogentes e de ordem pública;
>
> III – boa-fé: entendida como a exigência de que as partes atuem com honestidade, transparência, probidade, cooperação e lealdade durante a formação, a execução e a resolução dos contratos digitais;
>
> IV – equivalência funcional: com o entendimento de que os contratos digitais possuem a mesma validade legal que os contratos tradicionais e analógicos, desde que cumpridos os requisitos legais para sua formação;
>
> V – segurança jurídica: com a garantia de proteção aos direitos das partes envolvidas, assegurando a clareza, a precisão e a integridade dos termos acordados;
>
> VI – função social do contrato: nos termos do que está assegurado nos arts. 421 e 2.035, parágrafo único, deste Código.

A imaterialidade é inerente aos contratos digitais e refere-se ao fato de que os contratos digitais são formados e armazenados por meios eletrônicos, sem a necessidade de contrato físico, destacando a sua natureza imaterial e intangível. Contudo, em contratos dessa natureza, é indispensável a garantia da autenticidade e da integridade dos docu-

mentos que, em geral, são asseguradas por meio de assinaturas eletrônicas e tecnologias como o *blockchain*.

O princípio da autonomia privada assegura a liberdade das partes na criação de negócios jurídicos digitais, desde que estes não contrariem normas cogentes e de ordem pública e abre a possibilidade para escolha dos meios digitais que forem mais adequados para celebração do contrato digital. Já o princípio da boa-fé objetiva desempenha papel central nas relações contratuais. Em contratos digitais, nos quais a imaterialidade é característica, tal princípio e seus deveres anexos reforçam a atuação das partes de forma honesta, íntegra e leal.

Já o princípio da boa-fé desempenha papel central nas relações contratuais. Em contratos digitais, nos quais a imaterialidade é característica, tal princípio e seus deveres anexos reforçam a atuação das partes de forma honesta, íntegra e leal.

O princípio da equivalência funcional, por sua vez, estabelece que os contratos digitais têm a mesma validade legal dos contratos tradicionais, desde que observados os requisitos legais para a formação dos primeiros. Esse conceito já está consagrado em legislações internacionais, como no Regulamento eIDAS da União Europeia e na Lei Modelo da UNCITRAL sobre Comércio Eletrônico. A segurança jurídica nos contratos digitais está diretamente ligada à confiabilidade dos meios tecnológicos utilizados, como assinaturas eletrônicas, criptografia e blockchain, proporcionando integridade, clareza e precisão dos contratos digitais e garantindo a sua imutabilidade e o acesso aos registros de sua celebração.

Importante notar que o princípio da função social do contrato, consagrado nos arts. 421 e 2.035 do Código Civil, também se aplica aos contratos digitais. Em contratos digitais, a função social pode ser interpretada de diversas maneiras, como a proteção ao consumidor em transações on-line e a promoção de relações justas em plataformas digitais, em que o poder de negociação das partes pode ser desequilibrado tanto pelo fato de as transações B2C quanto pelo fato de as partes não terem poder sobre a programação e funcionalidade das plataformas digitais nas quais os contratos são efetuados. A função social também implica que as plataformas e tecnologias utilizadas nas contratações digitais devem promover um ambiente inclusivo e acessível.

A adaptação das regras tradicionais de contratos ao ambiente digital traz alguns desafios, como, por exemplo, a segurança jurídica em relação à identificação das partes e à integridade dos documentos digitais. Especificamente, em se tratando de negócios jurídicos caracterizados por maior densidade econômica, maior complexidade procedimental ou mesmo por um grau de risco considerável, verifica-se, não raras vezes, a imposição de formalidades adicionais pelo legislador. Tais formalidades podem envolver desde a obrigatoriedade de emprego da certificação digital vinculada à ICP-Brasil até a implementação de processos de verificação de identidade das partes ainda mais estritos

e meticulosos. Essas exigências, cuja incidência se revela especialmente acentuada em transações de conteúdo sensível – como operações financeiras de grande porte, cessões de direitos patrimoniais ou negócios que tenham por objeto ativos relacionados à propriedade intelectual –, têm como efeito, a partir do atendimento de seus requisitos, viabilizar que o contrato eletrônico venha a ostentar grau de robustez jurídica e de eficácia probatória equiparável àquele reconhecido aos documentos físicos tradicionalmente utilizados, preservando, por conseguinte, a necessária segurança jurídica das relações firmadas no ambiente digital. O artigo destaca a necessidade de adaptação das normas tradicionais do direito contratual às especificidades do ambiente digital, ao mesmo tempo que mantém os princípios essenciais de validade contratual, como a manifestação de vontade, a licitude do objeto e o cumprimento dos requisitos sobre a forma.

Além disso, nos termos do art. 2027-AU, ao admitir formas alternativas de manifestação de vontade, como cliques ou marcações em interfaces digitais, o dispositivo do Projeto de Lei no. 4, de 2025, reforça a tendência de reconhecimento das novas tecnologias e dos métodos contemporâneos de formação contratual como válidos, desde que observados os direitos das partes e garantida a segurança jurídica[33]. Nesse contexto, como se verá no próximo item, o atendimento aos requisitos legais aplicáveis às assinaturas eletrônicas e aos procedimentos de identificação dos contratantes torna-se elemento indispensável para assegurar a validade, a eficácia e a confiabilidade da transação realizada em ambiente digital.

O Projeto de Lei nº 4, de 2025[34], também estabelece, em seu art. 2.027-AR, os parâmetros específicos para a interpretação dos contratos digitais, destacando cinco elementos essenciais: funcionalidade conjunta, compatibilidade, interoperabilidade, durabilidade e uso comum e esperado.

A análise interpretativa dos contratos digitais exige uma compreensão integrada de sua funcionalidade conjunta, isto é, da maneira como os diferentes componentes técnicos e jurídicos interagem para produzir os efeitos desejados pelas partes. No caso dos *smart contracts*, por exemplo, tal funcionalidade resulta da combinação entre o código-fonte, a infraestrutura da *blockchain* e, quando presentes, os oráculos externos responsáveis pelo fornecimento de dados essenciais à execução automatizada das cláusulas contratuais. A lógica que orienta esses contratos é de uma automação autoexecutável, em que o papel de cada elemento técnico se torna decisivo para a concretização dos efeitos contratuais pretendidos (Santos, 2022, p. 50-55), o que demanda uma abordagem interpretativa que considere o contrato como um sistema integrado, articulando as camadas técnicas e jurídicas de modo a assegurar a realização harmônica dos objetivos inicialmente pactuados.

33 "Art. 2027-AS. O contrato formalizado por meio digital é considerado celebrado quando: I - as partes manifestarem claramente a sua intenção de contratar, podendo a manifestação ser expressa por cliques, seleção de opções em interfaces digitais, assinaturas eletrônicas, ou por outros meios que demonstrem claramente a concordância com os termos propostos; II - o objeto do contrato for lícito, possível, determinado ou determinável; III - o contrato atender aos requisitos de forma e de solenidade previstos em lei, quando for o caso, incluindo a identificação das partes e a assinatura eletrônica, quando necessária."

34 "Art. 2.027-AR. Na interpretação dos contratos digitais, devem ser considerados a sua funcionalidade conjunta, a compatibilidade, a interoperabilidade, a durabilidade e o seu uso comum e esperado."

Paralelamente, o critério da compatibilidade exige que a interpretação dos contratos digitais se preocupe com a coerência interna entre os diferentes sistemas tecnológicos envolvidos na sua execução, preocupação essa que se mostra especialmente relevante quando se trata de *smart contracts* desenvolvidos em blockchains públicas, nas quais a integração com outras aplicações, tokens e protocolos de segurança depende de uma sintonia fina entre a linguagem de programação, a lógica operacional e as exigências jurídicas externas.

No mesmo sentido, a questão da interoperabilidade impõe à interpretação a consideração sobre a capacidade do contrato de dialogar não apenas com diferentes ambientes tecnológicos, mas também com múltiplos sistemas jurídicos, sendo fundamental avaliar se há efetiva comunicação entre plataformas, aplicações e bancos de dados heterogêneos. A literatura especializada diferencia a interoperabilidade de serviços – que envolve a integração de vários sistemas, aplicações e serviços desenvolvidos de forma independente, com superação de barreiras sintáticas e semânticas (Lazai Júnior; Justus; Santos, 2020) – da interoperabilidade de dados, que diz respeito à gestão de diferentes modelos de dados e linguagens de consulta para viabilizar o compartilhamento de informações entre sistemas diversos, inclusive aqueles localizados em máquinas e ambientes operacionais distintos (Lazai Júnior; Justus; Santos, 2020). A ausência de interoperabilidade compromete não apenas a execução eficiente do contrato, mas também a própria possibilidade de controle judicial posterior (Santos, 2022, p. 92–106), razão pela qual a interpretação deve buscar soluções que preservem a conexão entre as múltiplas camadas técnicas e jurídicas envolvidas.

Outro aspecto a ser considerado é a durabilidade, elemento que demanda uma avaliação da estabilidade das condições técnicas e normativas que sustentam a eficácia contratual ao longo do tempo. A imutabilidade das *blockchains*, embora ofereça um fator de segurança quanto à integridade do contrato, também gera preocupações relacionadas à rigidez excessiva e à ausência de mecanismos eficazes de revisão ou adaptação, sobretudo diante de alterações fáticas ou normativas supervenientes. Nesse contexto, existe o risco de que a falta de ferramentas de modificação pós-contratual acarrete dificuldades de adequação dos contratos inteligentes às novas realidades (Gobbo, 2022, p. 185–190), de modo que a interpretação deve buscar um equilíbrio entre a segurança jurídica e a necessária flexibilidade para ajustes futuros.

O Projeto de Lei nº 4, de 2025, trata ainda da validação jurídica dos contratos celebrados por meio de aplicativos digitais, estabelecendo que são válidos e eficazes desde que atendam aos requisitos legais do Código Civil[35]. Nos termos do parágrafo único, aplicativo digital abrange qualquer plataforma, *software* ou sistema eletrônico que permita a celebração, gestão e execução de contratos, com foco na intermediação de bens não fungíveis ou imateriais.

35 "Art. 2.027-AV. O contrato celebrado por aplicativo digital é válido e eficaz, se atendidos os requisitos legais previstos neste Código. Parágrafo único. Para fins deste artigo, entende-se por aplicativo digital qualquer plataforma, software ou sistema eletrônico que permita a celebração, gestão e execução de contratos que tenham por objeto a intermediação do uso, gozo e fruição de coisa não fungível ou imaterial."

O art. 2027-AV começa estabelecendo que os contratos celebrados por meio de aplicativos digitais são válidos e eficazes desde que cumpram os requisitos previstos no Código Civil. Isso significa que, assim como os contratos celebrados em formatos tradicionais (escritos ou verbais), os contratos digitais devem respeitar os elementos essenciais jurídicos com: a) Consentimento livre e expresso das partes; b) Objeto lícito, possível, determinado ou determinável; c) Capacidade das partes contratantes.

Com a crescente popularidade de plataformas que permitem a gestão remota de contratos, como os aplicativos móveis, *e-commerce* e *marketplaces*, o artigo confirma que as transações realizadas por esses meios possuem a mesma força vinculante dos contratos celebrados em papel ou por outros métodos mais tradicionais.

O parágrafo único do art. 2027-AV define o conceito de aplicativo digital, abrangendo qualquer plataforma, *software* ou sistema eletrônico que permita a celebração, gestão e execução de contratos.

O ponto de destaque do parágrafo único é o foco na intermediação do uso, gozo e fruição de coisas não fungíveis ou imateriais. A referência a bens não fungíveis sugere a inclusão de ativos digitais, como, por exemplo, NFTs (*non-fungible tokens*), que têm ganhado grande relevância no ambiente digital. Esses ativos não são substituíveis por outros de igual natureza, o que os diferencia dos bens fungíveis, como dinheiro ou mercadorias comuns. O contrato digital, neste contexto, pode regular o uso de itens como obras de arte digitais, músicas, patentes ou qualquer outro tipo de bem intangível e único.

Além disso, a menção a bens imateriais amplia o escopo dos contratos, abrangendo, por exemplo, licenças de *software*, propriedade intelectual, direitos autorais e outros ativos intangíveis que se tornaram parte integrante das economias digitais. Nesse sentido, o artigo reconhece o papel central da economia digital e a necessidade de adequar o direito contratual às realidades emergentes, em que a fruição de direitos sobre bens imateriais é cada vez mais comum.

O Projeto de Lei[36] trata da definição e dos requisitos de segurança aplicáveis aos con-

36 "Art. 2.2027-AU. São considerados contratos inteligentes (smart contracts) aqueles nos quais algumas ou todas as obrigações contratuais são definidas ou executadas automaticamente por meio de um programa de computador, por meio da utilização de sequência de registros eletrônicos de dados e garantindo-se a integridade e a precisão de sua ordenação cronológica.

Parágrafo único. O fornecedor que utiliza contratos inteligentes ou, na sua ausência, a pessoa cujo comércio, negócio ou profissão envolva a sua implementação para terceiros, no contexto da execução de um acordo ou parte dele e ao disponibilizar dados, deve garantir que tais contratos cumpram os seguintes requisitos:

I - Robustez e controle de acesso, para assegurar que o contrato inteligente foi projetado para oferecer mecanismos de controle de acesso e um grau muito elevado de segurança a fim de evitar erros funcionais e resistir à manipulação por terceiros;

II - Término seguro e interrupção, para garantir que exista um mecanismo para encerrar a execução contínua de transações e que o contrato inteligente inclua funções internas capazes de reiniciar ou instruir o contrato a parar ou interromper a operação, especialmente para evitar futuras execuções acidentais;

III - Auditabilidade, com arquivamento de dados e continuidade, para garantir, em circunstâncias em que um

tratos inteligentes (*smart contracts*), destacando as responsabilidades do fornecedor ou implementador desses contratos e os mecanismos necessários para garantir a execução correta e segura deles.

Nesse mesmo sentido, é a definição caput do artigo 2.2027-AU que trata dos contratos inteligentes como sendo aqueles em que algumas ou todas as obrigações contratuais são definidas ou executadas automaticamente por meio de um programa de computador. Esse conceito é central no uso de blockchain e outras tecnologias descentralizadas, em que os *smart contracts* são programados para executar ações automaticamente, sem a necessidade de intervenção humana direta, uma vez que as condições preestabelecidas no código sejam atendidas.

Conforme salientam Eduardo Talamini e André Guskow Cardoso (2023), na sua origem, os contratos inteligentes não estavam ligados nem dependiam da tecnologia blockchain. De fato, quando a ideia de contratos inteligentes surgiu, no início dos anos 1990, a tecnologia blockchain ainda não havia sido criada, o que ocorreu por volta de 2008. Uma das funcionalidades que se tornaram possíveis com o desenvolvimento da tecnologia blockchain é a criação de contratos inteligentes autoexecutáveis. Esses contratos são constituídos por códigos de programação que executam determinadas ações uma vez que certas condições sejam atendidas. Os contratos inteligentes são armazenados nos blocos de uma rede *blockchain*, e suas execuções subsequentes também são registradas nesses blocos. Nesse sentido, os autores afirmam que:

> O uso da tecnologia blockchain para a elaboração e execução de smart contracts produziu uma verdadeira revolução no conceito dos smart contracts. Embora, como dito, a noção já existisse antes mesmo do desenvolvimento da tecnologia blockchain,foi apenas com a evolução desta última que a implantação e utilização dos smart contracts passou a ser factível e mais difundida. Isso se deu principalmente em razão das peculiaridades e dos atributos da tecnologia blockchain. As características peculiares da tecnologia blockchain são comuns a todas as redes, em maior ou menor grau. A arquitetura peculiar da tecnologia blockchain apresenta algumas decorrências específicas. (Talamini; Cardoso, 2023)

O parágrafo único do referido artigo atribui ao fornecedor que adota contratos inteligentes, bem como àqueles que os desenvolvem ou operacionalizam para terceiros, a obrigação de assegurar que tais instrumentos atendam a padrões mínimos de segurança e controle. Tal exigência objetiva proteger os contratantes, reconhecendo a complexidade técnica dos

---

contrato inteligente precise ser encerrado ou desativado, a possibilidade de arquivar os seus dados transacionais, a sua lógica e o seu código a fim de manter-se o registro dos dados das operações passadas;

IV - Controle de acesso, para assegurar que o contrato inteligente esteja protegido por meio de mecanismos rigorosos de controle de acesso nas camadas de governança; e

V - Consistência, para garantir a conformidade com os termos do acordo que o contrato inteligente executa."

smart contracts e a dificuldade que pessoas sem formação específica na área de tecnologia têm em compreender plenamente seu funcionamento e os riscos envolvidos, uma vez que a assimetria de informação e a falta de compreensão do código por parte dos usuários finais são fatores que elevam a necessidade de responsabilização daquele que disponibiliza ou implementa o contrato.

De acordo com o parágrafo único, os contratos devem cumprir os seguintes requisitos objetivos:

> I – robustez e controle de acesso, para assegurar que o contrato inteligente foi projetado para oferecer mecanismos de controle de acesso e um grau muito elevado de segurança a fim de evitar erros funcionais e resistir à manipulação por terceiros;
>
> II – término seguro e interrupção, para garantir que exista um mecanismo para encerrar a execução contínua de transações e que o contrato inteligente inclua funções internas capazes de reiniciar ou instruir o contrato a parar ou interromper a operação, especialmente para evitar futuras execuções acidentais;
>
> III – auditabilidade, com arquivamento de dados e continuidade, para garantir, em circunstâncias em que um contrato inteligente precise ser encerrado ou desativado, a possibilidade de arquivar os seus dados transacionais, a sua lógica e o seu código a fim de manter-se o registro dos dados das operações passadas;
>
> IV – controle de acesso, para assegurar que o contrato inteligente esteja protegido por meio de mecanismos rigorosos de controle de acesso nas camadas de governança; e
>
> V – consistência, para garantir a conformidade com os termos do acordo que o contrato inteligente executa.

3.8 Assinaturas eletrônicas

O texto abaixo está contido no Capítulo IX do Livro Direito Civil Digital, do Projeto de Lei nº 4, de 2025, intitulado "Assinaturas eletrônicas".

CAPÍTULO IX - ASSINATURAS ELETRÔNICAS

Art. 2027-AW. São modalidades de assinaturas eletrônicas, para os devidos fins deste Código:

I - assinatura eletrônica simples:

a) a que permite identificar o seu signatário;

b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela chave pública brasileira Ideal Customer Profile--Brasil-ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:

a) estar associada ao signatário de maneira unívoca;

b) utilizar dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;

c) estar relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;

III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

§ 1º A assinatura digital qualificada comprova a autoria do documento, vinculando-o ao titular do respectivo certificado.

§ 2º A assinatura, por si só, não constitui prova da capacidade ou da ausência de vícios na manifestação de vontade, o que pode ser demonstrado por qualquer interessado.

> Art. 2027-AX. Salvo disposição legal em sentido contrário, a validade de documentos constitutivos, modificativos ou extintivos de posições jurídicas que produzam efeitos perante terceiros depende de assinatura qualificada.

3.8.1 Abordagem teórica da temática

As assinaturas eletrônicas passaram a ocupar posição de destaque no processo de formalização dos contratos digitais, sendo atualmente reconhecidas como uma das formas mais seguras e confiáveis, do ponto de vista técnico, para a comprovação da manifestação livre, consciente e inequívoca da vontade das partes contratantes. No ordenamento jurídico brasileiro, sua incorporação normativa deu-se, de forma inaugural, com a edição da Medida Provisória nº 2.200-2/2001, a qual instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e, com isso, conferiu tratamento jurídico diferenciado, notadamente em relação à assinatura eletrônica qualificada. Esta última, por sua natureza técnica e jurídica, tem como propósito fundamental assegurar, com elevados padrões de segurança, tanto a autenticidade quanto a integridade dos documentos digitais, elementos indispensáveis à sua validade jurídica e à sua força probante.

Essa sistemática encontra-se fundamentada também na Lei nº 14.063/2020, que disciplina as assinaturas eletrônicas no Brasil, classificando-as em simples (art. 4º, I), avançadas (art. 4º, II) e qualificadas (art. 4º, III). A escolha entre uma ou outra modalidade depende do grau de segurança exigido pela natureza do contrato, o que permite ao ordenamento contemplar desde operações mais simples – cuja aceitação pode ocorrer por meio de um clique – até negócios jurídicos que exigem o emprego de uma assinatura eletrônica qualificada para assegurar sua integridade e autenticidade.

A segurança é obtida pelo uso de assinaturas eletrônicas, as quais são feitas por meio de criptografia assimétrica, criando uma chave ao remetente e outra ao destinatário, uma privada e outra pública, respectivamente. Além da criptografia assimétrica, os certificados digitais também são fundamentais para que se tenha certeza de que a assinatura é legítima e consistem em um atestado de quem assinou é realmente quem diz ser emitido por um terceiro de confiança de forma presencial. Aqui, o objetivo é identificar qualquer alteração no documento digital e assegurar a autenticidade da assinatura.

É importante mencionar que assinatura eletrônica se diferencia da assinatura digital. As assinaturas eletrônicas são feitas pela confirmação de um meio eletrônico, como, por exemplo, um computador, e esse conceito abrange assinaturas digitais, por reconhecimento de IP, *tokens*, biometria, entre outros. Não se exige certificação digital das partes envolvidas. Já a assinatura digital é feita de forma virtual, mas carregada de um nível extra de segurança e confiabilidade, haja vista que possuem certificado emitido pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), composta por criptografia. Assinaturas digitais são um tipo de assinatura eletrônica, implementadas por meio do uso de criptografia assimétrica.

Além disso, existem assinaturas eletrônicas que utilizam certificados por outros meios, que não a ICP-Brasil, são as chamadas assinaturas eletrônicas avançadas. A comprovação de legitimidade e autoria do documento eletrônico admite outros meios, desde que aceito pelas partes envolvidas. Esse tipo de assinatura utiliza dados do signatário de forma que quaisquer alterações posteriores à sua assinatura podem ser identificadas.

3.8.2 Experiências normativas do direito estrangeiro e transnacional

3.8.2.1 Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL)

A UNCITRAL, já desde 2001, estabeleceu as bases normativas com a Model Law on Electronic Signatures, difundindo os princípios de equivalência funcional, neutralidade tecnológica e reconhecimento jurídico das assinaturas eletrônicas.

3.8.2.2 União Europeia

O Regulamento eIDAS (Electronic Identification and Trust Services – Regulamento (UE) N.º 910/2014) (União Europeia, 2014) estabelece um quadro legal para a identificação eletrônica e os serviços de confiança para transações eletrônicas no mercado interno da União Europeia.

Sobre as assinaturas eletrônicas, o regulamento eIDAS categoriza as assinaturas eletrônicas em três diferentes níveis: simples, avançadas e qualificadas –, escalonados em razão de seu nível de segurança e confiabilidade e estabelecendo que as assinaturas eletrônicas qualificadas impõem os mesmos efeitos jurídicos das assinaturas manuscritas.

3.8.2.3 Síntese analítica das experiências normativas de direito transnacional

No cenário internacional, a UNCITRAL, já desde 2001, estabeleceu as bases normativas com a *Model Law on Electronic Signatures*, difundindo os princípios de equivalência funcional, neutralidade tecnológica e reconhecimento jurídico das assinaturas eletrônicas.

Na União Europeia, o Regulamento eIDAS (910/2014) serve como principal referência. Assim como o PL 4/2025, o eIDAS distingue três níveis de assinatura: simples, avançada e qualificada. A assinatura qualificada europeia, emitida por prestadores autorizados, possui o mesmo valor jurídico de uma assinatura manuscrita em todos os Estados-Membros, além de integrar um sistema de reconhecimento mútuo entre países.

O Projeto de Lei nº 4, de 2025, consolida e atualiza o regime jurídico das assinaturas eletrônicas no Brasil. Pela primeira vez, o Código Civil passa a disciplinar expressamente a matéria, incorporando a classificação trinária de assinaturas: simples, avançada e qualificada. As assinaturas qualificadas, com certificado da ICP-Brasil, passam a ter força plena de prova da autoria documental e, salvo exceções legais, são exigidas para do-

cumentos que produzam efeitos perante terceiros. Portanto, aproxima o regime brasileiro das práticas normativas internacionais, especialmente do modelo europeu, ao adotar um sistema escalonado de segurança e presunção de validade, mas preservando peculiaridades locais como a centralidade da ICP-Brasil na emissão das assinaturas qualificadas.

3.8.3 Estudos de caso

3.8.3.1 Brasil: Recurso Especial nº 1.495.920

A título de análise jurisprudencial para melhor compreensão da aplicação da certificação da assinatura virtual, o REsp 1.495.920/DF julgado pela 3ª Turma do Superior Tribunal de Justiça, julgado em 15 de maio de 2018 e relatado pelo ministro Paulo de Tarso Severino, tratou da divergência sobre a executividade de um contrato de mútuo assinado eletronicamente, mas com a ausência da assinatura de duas testemunhas. O ministro analisou a questão da eficácia executiva do título da seguinte forma:

> Deste todo interpretativo, tem-se a concluir que, em regra, exige-se as testemunhas em documento físico privado para que seja considerado executivo, mas excepcionalmente, poderá ele dar azo a um processo de execução, sem que se tenha cumprido o requisito formal estabelecido no art. 585, II, do CPC/73, qual seja, a presença de duas testemunhas, entendimento este que estou em aplicar aos contratos eletrônicos, desde que observadas as garantias mínimas acerca de sua autenticidade e segurança. O contrato eletrônico, em face de suas particularidades, por regra, tendo em conta a sua celebração à distância e eletronicamente, não trará a indicação de testemunhas, o que, entendo, não afasta a sua executividade. Não há dúvidas de que o contrato eletrônico, na atualidade, deve ser, e o é, colocado em evidência pela sua importância econômica e social, pois a circulação de renda tem-no, no mais das vezes, como sua principal causa. [...] Acerca dos requisitos do contrato eletrônico, ou para que sejam utilizados como prova, Patrícia Peck lembra exigirem: "a certificação eletrônica, assinatura digital, autenticação eletrônica, para manter a autenticidade e integridade do documento, conforme o meio que foi utilizado para a sua realização." Pela conformação dos contratos eletrônicos, o estabelecimento da necessidade de conterem a assinatura de 2 testemunhas para que sejam considerados executivos, dificultaria, por deveras, a sua satisfação. Se, como ressalta a referida doutrinadora, agrega-se a eles autenticidade e integridade mediante a certificação eletrônica, utilizando-se a assinatura digital devidamente aferida por autoridade certificadora legalmente constituída, parece-me mesmo desnecessária a assinatura das testemunhas. (Superior Tribunal de Justiça, 2018)

O entendimento da 3ª Turma foi positivado pela Lei nº 14.620/2023 ao dispor que "títulos executivos constituídos ou atestados por meio eletrônico, é admitida qualquer

modalidade de assinatura eletrônica prevista em lei, dispensada a assinatura de testemunhas quando sua integridade for conferida por provedor de assinatura".

A assinatura digital, entretanto, já é considerada um requisito indispensável para a validade dos contratos eletrônicos, conforme manifestado pelo STJ nos autos do REsp 1.495.920:

> A assinatura digital de contrato eletrônico tem a vocação de certificar, através de terceiro desinteressado (autoridade certificadora), que determinado usuário de certa assinatura a utilizara e, assim, está efetivamente a firmar o documento eletrônico e a garantir serem os mesmos os dados do documento assinado que estão a ser sigilosamente enviados. (Superior Tribunal de Justiça, 2018)

3.8.3.2 Brasil: Recurso Especial nº 2.022.423

O uso do e-mail como meio de manifestação da vontade para a celebração de contratos tornou-se uma prática comum e agora é potencialmente reconhecida como uma forma válida de celebração. Em que pese não oferecer o mesmo nível de segurança das assinaturas eletrônicas avançadas ou qualificadas, a formalização dele se dá a partir da recepção da aceitação pelo proponente (Enunciado 173 do CJF). Isso porque a comunicação não ocorre de forma imediata (Tartuce, 2023) – entre ausentes – de modo que se aplica a teoria da agnição, na subteoria da recepção. Nesse sentido, no julgamento do Recurso Especial n. 2.022.423-RS, relatado pela ministra Nancy Andrighi, a 3ª Turma do STJ, por unanimidade, entendeu que não se pode presumir que a notificação enviada por e-mail tenha atingido a finalidade de informar o devedor.

> CIVIL. DIREITO PROCESSUAL CIVIL. BUSCA E APREENSÃO REGIDA PELO DECRETO-LEI Nº 911/1969. MODIFICAÇÃO INTRODUZIDA NO DECRETO-LEI Nº 911/1969 PELA LEI Nº 13.043/2014. FINALIDADE DE FACILITAR A COMPROVAÇÃO DA MORA PELO CREDOR E DE DESBUROCRATIZAR O PROCEDIMENTO. SIMPLES ENVIO DE CARTA REGISTRADA COM AVISO DE RECEBIMENTO. INTERPRETAÇÃO EXTENSIVA PARA PERMITIR QUE A CONSTITUIÇÃO EM MORA OCORRA MEDIANTE ENVIO DE E-MAILAO DEVEDOR. IMPOSSIBILIDADE. MODALIDADE NÃO AUTORIZADA PELO LEGISLADOR. CIÊNCIA INEQUÍVOCA A RESPEITO DO RECEBIMENTO, LEITURA E CONTEÚDO QUE DEMANDARIA ATIVIDADE INSTRUTÓRIA INCOMPATÍVEL COM O RITO ESPECIAL DO DECRETO-LEI Nº 911/1969.
>
> [...]
>
> 2- O propósito recursal consiste em definir se, em ação de busca e apreensão regida pelo Decreto-Lei nº 911/1969, é admissível a comprovação da mora do réu mediante o envio da notificação extrajudicial por correio eletrônico (e-mail).
>
> [...]

> 4- Se é verdade que, na sociedade contemporânea, tem crescido o uso de ferramentas digitais para a prática de atos de comunicação de variadas naturezas, não é menos verdade que o crescente uso da tecnologia para essa finalidade tem de vir acompanhado de regulamentação que permita garantir, minimamente, que a informação transmitida realmente corresponde aquilo que se afirma estar contida na mensagem e de que houve o efetivo recebimento da comunicação pelo seu receptor.
>
> [...]
>
> 8- Descabe cogitar a possibilidade de reconhecer a validade da notificação extrajudicial enviada somente por correio eletrônico porque teria ela atingido a sua finalidade, na medida em que a ciência inequívoca de seu recebimento pressuporia o exame de uma infinidade de aspectos relacionados à existência de correio eletrônico do devedor fiduciante, ao efetivo uso da ferramenta pelo devedor fiduciante, a estabilidade e segurança da ferramenta de correio eletrônico e a inexistência de um sistema de aferição que possua certificação ou regulamentação normativa no Brasil, de modo a permitir que as conclusões dele advindas sejam admitidas sem questionamentos pelo Poder Judiciário.

3.8.4 Tratamento normativo em vigor e propostas legislativas nacionais sobre o instituto

3.8.4.1 Medida Provisória nº 2.200-2/2001

No Brasil, em 2001, a Medida Provisória n. 2.200-2 (Brasil, 2001) implementou a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e transformou o Instituto Nacional de Tecnologia da Informação em autarquia. A ICP-Brasil permitiu que assinaturas eletrônicas tivessem certificados digitais. O Código Civil de 2002, mesmo que posterior a essa medida provisória, não versou sobre a assinatura eletrônica.

A Medida Provisória n. 2.200-2 instituiu, em seu art. 1º, a ICP-Brasil como ferramenta de autenticação de assinaturas eletrônicas que garante autenticidade, validade jurídica e integridade nos documentos por meio de certificados digitais. Já em seu art. 2º, está disposto que a ICP-Brasil é regida pela "Autoridade Certificadora Raiz - Ac Raiz", pelas "Autoridades Certificadoras" e pelas "Autoridades De Registro". A AC Raiz confere aos usuários uma maior segurança na certificação digital, uma vez que possui um mecanismo de traçar os certificados digitais até que se chegue ao certificado originário da AC Raiz.

Conforme citado previamente, a Medida Provisória nº 2.200-2/2001 criou a ICP-Brasil e regulamentou os certificados digitais para documentos e transações eletrônicas. A norma mostrou-se um marco fundamental no regimento da integridade de contratos eletrônicos no Brasil, haja vista que atribuiu ao Governo Federal responsabilidade pela estruturação dela, com uma hierarquia de certificação que vai desde um Comitê Gestor até Autoridades Certificadoras de Registro.

Desde a edição da medida, é possível a equiparação da assinatura eletrônica qualificada à assinatura manuscrita, desde que emitida no âmbito da ICP-Brasil, deve ser considerada documento particular nos termos do art. 219 do Código Civil, tendo em vista a paráfrase do art. 10, §1º, da MP n. 2.200-2/2001 ao citado artigo do Código Privado:

> Art. 10 (...)
>
> § 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil (atual artigo 219 do CC).

3.8.4.2 Lei nº 14.063/2020

As assinaturas eletrônicas foram reconhecidas legalmente no ordenamento jurídico brasileiro pela Lei nº 14.063/2020 (Brasil, 2020), a qual apresenta requisitos para o uso de assinaturas eletrônicas instituídas entre pessoas e instituições privadas com entes públicos ou entre os entes públicos. O art. 4º da referida lei dispõe sobre a classificação dos tipos de assinaturas:

> Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:
>
> I - assinatura eletrônica simples:
>
> a) a que permite identificar o seu signatário;
>
> b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;
>
> II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP--Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:
>
> a) está associada ao signatário de maneira unívoca;
>
> b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;
>
> c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;
>
> III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.
>
> § 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos.

§ 2º Devem ser asseguradas formas de revogação ou de cancelamento definitivo do meio utilizado para as assinaturas previstas nesta Lei, sobretudo em casos de comprometimento de sua segurança ou de vazamento de dados.

3.8.5 Comentários sobre o texto do projeto da reforma do Código Civil

O Projeto de Lei nº 4, de 2025, sistematiza o tratamento normativo das assinaturas eletrônicas, que era tratado de forma dispersa.

A Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), criando as bases da certificação digital no país. Posteriormente, a Lei nº 14.063/2020 disciplinou o uso das assinaturas eletrônicas nas interações com o poder público e introduziu a classificação das assinaturas em três categorias: simples, avançada e qualificada, bem como inovou ao permitir que documentos eletrônicos, devidamente verificados quanto à autoria e integridade, tenham força executiva mesmo sem a necessidade de testemunhas.

Com o Projeto de Lei nº 4, de 2025, essa estrutura normativa é consolidada e inserida no Código Civil, incorporando expressamente a classificação trinária já prevista na Lei nº 14.063/2020, inspirada no modelo do Regulamento Europeu eIDAS.

Além de reforçar esses conceitos, o PL 4/2025 também dialoga com a inovação da Lei nº 14.620/2023, ao confirmar que a exigência de testemunhas para fins de execução de contratos digitais pode ser dispensada, desde que a assinatura eletrônica qualificada assegure a integridade do documento.

Desta forma, o projeto atualiza o direito civil brasileiro para as demandas das transações digitais contemporâneas, a partir de parâmetros de segurança técnica e proteção jurídica adequados à complexidade das novas relações contratuais, bem como aproxima o Brasil das práticas regulatórias internacionais.

De acordo com o projeto de reforma do Código Civil, a assinatura digital é um dos requisitos necessários para a celebração de contratos digitais. Assim como a assinatura manuscrita, cumpre a função de identificação do signatário e de vinculá-lo ao conteúdo do contrato, conforme expresso no projeto quando se lê:

> Art. 2.027-AS. O contrato formalizado por meio digital é considerado celebrado quando:
>
> I - as partes manifestarem claramente a sua intenção de contratar, podendo a manifestação ser expressa por cliques, seleção de opções em interfaces digitais, assinaturas eletrônicas, ou por outros meios que demonstrem claramente a concordância com os termos propostos.

Desta forma, o projeto de reforma do Código Civil busca positivar essa prática que vem ocorrendo nas relações pessoais e mercantis, reconhecendo a validade das assinaturas eletrônicas como meio eficaz de manifestação de vontade.

CONSIDERAÇÕES FINAIS

04

4 CONSIDERAÇÕES FINAIS

O presente estudo está inserido na linha de pesquisa "Governança Digital e Inovação", explorou e abordou o impacto das transformações no ambiente digital e os desafios enfrentados na tentativa de regulamentá-lo, a partir da análise das propostas presentes no Livro Direito Civil Digital no âmbito da reforma do Código Civil. O estudo envolveu a análise das seguintes temáticas: a) Pessoa no ambiente digital: desindexação e exclusão de dados ou informações; b) Pessoa no ambiente digital: neurodireitos; c) Direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo; d) Patrimônio digital; e) A presença e a identidade de crianças e adolescentes no ambiente digital; f) Inteligência artificial: g) Celebração de contratos por meios digitais; e h) Assinaturas eletrônicas.

A partir de uma metodologia que conjugou revisão bibliográfica, análise documental, estudos de caso e comparação com experiências normativas internacionais, o trabalho identificou lacunas e desafios ainda presentes na legislação brasileira, além de apontar avanços trazidos pela proposta legislativa em exame, resumidos a seguir.

Da pessoa no ambiente digital: exclusão de dados pessoais, de informações e desindexação

O presente estudo trouxe um sólido referencial teórico que parte da constatação da crescente produção e circulação de dados pessoais na sociedade informacional, a partir de autores como Manuel Castells, Byung-Chul Han e Stefano Rodotá. Verificou-se que o cenário da sociedade de informação redimensionou o conceito de privacidade, que ultrapassa a mera proteção do segredo, incorporando o direito à autodeterminação informativa e o direito ao controle da circulação e da permanência das informações pessoais.

O estudo traz uma análise detalhada das políticas de moderação e remoção de conteúdo adotadas por grandes plataformas como Google, Meta, TikTok e X (antigo Twitter), que identificou uma adesão parcial às diretrizes estabelecidas no Projeto de Lei nº 4, de 2025, especialmente no tocante aos direitos de exclusão e desindexação previstos nos arts. 2.027-J a 2.027-L. De modo geral, observa-se que, embora haja canais de denúncia e de solicitação de remoção de conteúdo em todos os casos analisados, os procedimentos atualmente adotados pelas platafor-

mas ainda não alcançam o padrão normativo mais protetivo delineado pela proposta legislativa, especialmente no que se refere à fundamentação dos pedidos, à inversão do ônus da prova em certas hipóteses e à garantia de exclusão de conteúdos excessivamente prejudiciais, ainda que verídicos.

A análise das experiências normativas internacionais e transnacionais destacou a experiência da União Europeia, que, com o GDPR e a jurisprudência do TJUE (caso *Google Spain vs. Costeja González*), é referência mundial no tratamento de questões como desindexação e exclusão de dados e informações. Outras experiências normativas foram destacadas como do Reino Unido (*Data Protection Act* 2018), da Argentina e do Chile, revelando um panorama de abordagens semelhantes, com ênfase na tensão entre privacidade e liberdade de expressão. O estudo dessas experiências normativas permitiu verificar que o Projeto de Lei nº 4, de 2025, alinha-se claramente ao modelo europeu, reforçando a tutela da personalidade e a autodeterminação informativa.

Além disso, os estudos dos casos Chacina da Candelária, Aída Curi e dos recursos extraordinários, relacionados ao Orkut e ao Facebook (Temas 533 e 987 do STF), contribuíram para ilustrar os dilemas concretos enfrentados pelo Judiciário brasileiro que serviram de baliza para o texto do Projeto de Lei nº 4, de 2025.

O Capítulo II do Livro Direito Civil Digital preenche uma lacuna importante ao normatizar plataformas digitais com a previsão de critérios claros e objetivos para exclusão de dados e desindexação, já que o tratamento da matéria no Brasil se encontra fragmentado e lacunoso diante do tratamento conferido pela LGPD e pelo Marco Civil da Internet. Desta forma, o texto avança ao positivar o direito à desindexação como direito autônomo, bem como ao definir critérios e procedimentos objetivos para exclusão de dados e informações

Da pessoa no ambiente digital: neurodireitos

A evolução das neurociências e das neurotecnologias introduziu novas possibilidades de interação homem-máquina, como as interfaces cérebro-computador, ampliando riscos relacionados à privacidade mental, ao livre-arbítrio, à manipulação cognitiva e à igualdade no acesso a tecnologias de aprimoramento, com possibilidades de manipulação, exploração econômica e coleta indevida de neurodados.

Os estudos de caso como *Smt. Selvi vs. Karnataka* (Índia) e *Girardi vs. Emotiv Inc.* (Chile) ilustram que não se trata de uma abordagem meramente teórica, mas sim de questões que já estão chegando ao Judiciário e que envolvem o impacto direto das neurotecnologias sobre direitos fundamentais e temas como consentimento forçado, violação da privacidade mental e uso indevido de neurodados.

O estudo das experiências internacionais e transnacionais revelou que o Chile lidera a positivação dos neurodireitos ao nível constitucional. Já países como Espanha, França e organizações como OCDE e OEA avançam por meio de instrumentos de *soft law* ou cartas de princípios. Essas experiências apontam para a necessidade de um marco legal específico que assegure

governança ética, transparência, consentimento informado e proteção contra usos indevidos. Desta forma, o PL 4/2025 posiciona o Brasil em sintonia com os melhores padrões internacionais, inspirando-se nas práticas chilena e europeia, mas avançando ao reconhecer os neurodireitos de forma ampla dentro do Código Civil, com potencial para ser referência normativa na América Latina. O Brasil segue a tendência de regulamentação do tema e possui iniciativas normativas isoladas, como a Emenda Constitucional do Rio Grande do Sul, a PEC nº 29/2023 e os Projetos de Lei nº 1.229/2021, 522/2022 e 2.174/2023. Porém, há ainda uma lacuna no ordenamento jurídico que carece de uma legislação nacional consolidada e de eficácia geral para o tema.

Assim, o Projeto de Lei nº 4, de 2025, visa preencher uma lacuna legislativa relevante, criando um arcabouço jurídico centralizado e sistemático, que harmoniza os neurodireitos com os direitos da personalidade e estabelece bases sólidas para futuras regulamentações infraconstitucionais e setoriais, promovendo segurança jurídica, previsibilidade regulatória e proteção substancial à integridade mental.

Do direito ao ambiente digital transparente e seguro: plataformas digitais e moderação de conteúdo

As plataformas digitais passaram a desempenhar um papel central no fluxo de informações e na interação social, por meio de sua estrutura algorítmica, com influência sobre o discurso público, os comportamentos de consumo e até processos eleitorais.

O estudo das experiências normativas internacionais e transnacionais evidenciou que, no âmbito da União Europeia, com o Digital Services Act (DSA), a Regulamentação para a proteção da privacidade e dos dados, o Regulamento Geral de Proteção de Dados e o Digital Markets Act (DMA), entre outras, há um modelo de regulação robusta, com ênfase em deveres de transparência, responsabilidade escalonada e auditorias independentes. Já o Reino Unido avança com o Online Safety Act, enquanto os Estados Unidos mantêm um modelo fragmentado e fortemente influenciado pela Primeira Emenda, com discussões em torno da revisão da Seção 230 do Communications Decency Act. O PL 4/2025 se alinha sobretudo ao modelo europeu, ao criar um regime de responsabilidade progressiva para plataformas de grande alcance, adotando ferramentas de auditoria, avaliação de riscos e obrigações de transparência algorítmica.

Os estudos de caso evidenciaram que a temática é objeto de decisões judiciais em diversos países, e, no Brasil, os estudos sobre os Temas de Repercussão Geral no STF demonstram uma evolução jurisprudencial no sentido de revisar a suficiência do art. 19 do Marco Civil da Internet com destaque para os Temas 533 e 987 da repercussão geral, que reconheceram a insuficiência do regime de responsabilidade civil previsto no artigo em questão. O STF, ao declarar a inconstitucionalidade parcial do art. 19 do MCI, e admitiu a responsabilização dos provedores em casos de omissão diante de notificações, impulsionamento de conteúdo ilícito, uso de redes artificiais de disseminação e falhas sistêmicas na prevenção de danos. Assim, a proposta de reforma do Código Civil está alinhada à orientação fixada pelo STF, com um novo padrão regulatório sobre a responsabilidade civil e os deveres de governança das plataformas digitais.

Patrimônio digital

A abordagem teórica realizada sobre o patrimônio digital revelou a profunda transformação das categorias tradicionais do Direito Civil frente à digitalização da vida e à crescente relevância dos ativos digitais, por meio da "plataformização da vida" e da massificação do uso de dispositivos móveis que consolidaram o legado digital.

A análise das políticas das principais plataformas digitais (Apple, Facebook, Google, Instagram e X/Twitter) demonstrou que, embora haja um reconhecimento crescente da importância do legado digital, o tratamento da matéria ainda é fragmentado e baseado em soluções unilaterais definidas por cada provedor, o que reforça a necessidade de uma regulamentação legal nacional, como a proposta pelo PL 4/2025.

As experiências normativas estrangeiras revelam que a regulamentação sucessória do patrimônio digital é uma tendência, com certa semelhança de tratamento da matéria. Em alguns países, como a Alemanha, há a transmissão automática dos ativos digitais aos herdeiros, salvo disposição em contrário do falecido e em algumas hipóteses legais previstas. Em sentido semelhante, a Espanha regulamentou a matéria. Assim, o Projeto de Lei nº 4, de 2025, representa um avanço ao preencher essa lacuna no ordenamento jurídico brasileiro, incorporando soluções que já vêm sendo implementadas em outros países.

Os estudos de caso sobre a sucessão de bens digitais revelaram diversos entendimentos sobre a temática. Na Alemanha, o *Bundesgerichtshof* reconheceu o direito dos herdeiros ao acesso integral à herança digital do falecido, com base na transmissibilidade contratual e patrimonial. Já, no Brasil, prevalece um cenário de decisões fragmentadas, influenciadas pelas especificidades de cada caso.

O Capítulo V do Projeto de Lei nº 4, de 2025, ao tratar do patrimônio digital, representa o reconhecimento dos ativos digitais como parte integrante do patrimônio das pessoas físicas e jurídicas, conferindo-lhes proteção jurídica específica. O estudo identificou outros projetos de lei que objetivam regulamentar aspectos relacionados ao patrimônio digital. Contudo, o Projeto de Lei nº 4, de 2025, oferece um tratamento normativo adequado à complexidade dos ativos digitais no contexto sucessório, pois adota uma classificação trinária dos bens digitais (econômicos, personalíssimos e híbridos), reconhecendo o patrimônio digital como uma nova dimensão da herança, compatível com os princípios constitucionais de proteção à dignidade, à privacidade e à autodeterminação informativa. A proposta avança ao regulamentar a transmissão hereditária desses bens com a garantia de que os titulares possam dispor sobre seus ativos digitais por meio de testamento, inclusive no que tange ao acesso às senhas e às contas pessoais.

A presença e a identidade de crianças e adolescentes no ambiente digital

O uso de dispositivos digitais por crianças e adolescentes traz benefícios importantes para o desenvolvimento educacional, social e cognitivo, mas também impõe riscos significativos à saúde física, emocional e ao desenvolvimento psicossocial.

A atuação das plataformas digitais foi analisada, com destaque para as políticas praticadas pela Meta. Verificou-se que a política da empresa em relação à proteção de crianças e de adolescentes no ambiente digital demonstra um avanço relevante na adoção de práticas alinhadas aos princípios de segurança, de privacidade e de bem-estar infantojuvenil, com o estabelecimento de configurações de privacidade mais restritivas por padrão até a limitação de interações entre adolescentes e adultos desconhecidos, bem como a filtragem de conteúdos sensíveis e a adoção de ferramentas de gerenciamento de tempo de uso.

O estudo das experiências normativas internacionais e transnacionais demonstrou que diversos países buscam garantir a proteção de crianças e adolescentes no ambiente digital com normatizações semelhantes. Merece destaque a regulamentação da União Europeia, que estabelece regras rígidas de proteção de dados e de proibição de publicidade direcionada e de avaliação de riscos específicos para menores. Na mesma linha, a Espanha trata da temática a partir de um conjunto de leis e regulamentos que criam diretrizes para a proteção da presença e da identidade de crianças e adolescentes no ambiente digital. O Reino Unido, por meio do *Online Safety Act* (2023), estabelece o dever de cuidado das plataformas, com a previsão de medidas preventivas desde o design, de maior controle sobre conteúdos acessíveis às crianças e aos adolescentes e de canais para denúncias. Verificou-se, portanto, que o Projeto de Lei nº 4, de 2025, segue essas mesmas linhas normativas, complementado as proteções previstas no ECA e na LGPD.

O tratamento normativo vigente no Brasil sobre a proteção de crianças e adolescentes no ambiente digital reflete uma evolução normativa orientada pela proteção integral e pelo superior interesse de crianças e de adolescentes por meio da Resolução CONANDA nº 245/2024, das Leis Estaduais nº 12.730/2007 e 18.058/2024 (São Paulo) e da recente Lei Federal nº 15.100/2025.

O Projeto de Lei nº 4, de 2025, ao prever normas específicas para o ambiente digital infantil, reforça a proteção integral já estabelecida pela Constituição Federal e pelo Estatuto da Criança e do Adolescente. A proposta consolida diretrizes como a implementação de sistemas de verificação etária, o desenvolvimento de produtos com design seguro, a vedação da publicidade direcionada e a proteção reforçada de dados pessoais, em sintonia com os direitos fundamentais à saúde, educação, privacidade e ao desenvolvimento seguro. Além disso, o projeto reconhece a vulnerabilidade ampliada de crianças e de adolescentes frente ao design persuasivo e ao modelo de negócios das plataformas digitais, com o reconhecimento da responsabilidade estatal e privada na garantia de um ambiente digital compatível com o estágio de desenvolvimento das crianças e dos adolescentes.

Inteligência artificial

O Projeto de Lei nº 4, de 2025, apesar de não regulamentar exaustivamente a inteligência artificial, o que não seria o seu objetivo, traz princípios gerais relevantes e regulamenta especificamente a crescente utilização da IA na geração de imagens, incluindo *deepfakes*, que expõe

a riscos no que diz respeito à proteção da imagem e à privacidade e tem sido um dos maiores desafios regulatórios no âmbito da inteligência artificial.

Verificou-se que as plataformas digitais vêm adotando medidas que refletem uma preocupação com o crescente compartilhamento de deepfakes, de forma a dar transparência quando houver o uso de inteligência artificial.

O estudo das experiências normativas internacionais e transnacionais trouxe o detalhamento da normatização da criminalização da produção e da divulgação de *deepfakes* não consensuais pela Austrália, pela União Europeia, pela China e pelos Estados Unidos.

A complexidade da temática da inteligência artificial na criação e na disseminação de conteúdos digitais foi percebida também nos estudos de caso, tanto no caso da campanha da Volkswagen, com a imagem da cantora Elis Regina, como em relação às decisões dos Tribunais Regionais Eleitorais (TREs) sobre *deepfakes* nas eleições de 2024.

Os dados levantados nesse estudo demostraram que há um crescente tratamento normativo da inteligência artificial no Brasil, como a recente promulgação da Lei nº 15.123/2025, que agrava a pena de violência psicológica praticada com IA e, no âmbito eleitoral, com a Resolução TSE nº 23.732/2024 que reforça o combate à desinformação e às *deepfakes*, exigindo rotulagem clara de conteúdos sintéticos e proibindo práticas enganosas que possam afetar o processo democrático. Além disso, diversos projetos de lei em tramitação apontam para um esforço legislativo coordenado de atualizar o Código Civil, o Código Penal e o Código de Defesa do Consumidor, bem como para criar um diploma normativo específico que regulamente a inteligência artificial no Brasil.

O Capítulo VII do PL 4/2025, como já dito anteriormente, prevê a necessidade de regulamentação específica futura para a inteligência artificial, mas avança ao estabelecer princípios fundamentais para o desenvolvimento e o uso de sistemas de IA, com foco na proteção da personalidade, na segurança jurídica e na prevenção de danos, por meio da obrigatoriedade de transparência, explicabilidade e supervisão humana nos processos automatizados, com destaque para regulação específica sobre a criação de imagens de pessoas vivas ou falecidas por meio de IA, impondo requisitos de consentimento, respeito à dignidade e vedação à exploração comercial não autorizada.

Da celebração de contratos por meios digitais

O advento dos contratos digitais nos leva a repensar os conceitos tradicionais da Teoria Geral dos Contratos diante da nova realidade das contratações digitais. Os contratos digitais não são uma nova espécie contratual e mantêm os requisitos clássicos de validade. Contudo, o meio digital pode atuar diferentemente na formação contratual e até na sua execução.

O estudo das experiências normativas estrangeiras e transnacionais permitiu verificar uma tendência no reconhecimento da validade jurídica dos contratos digitais e dos contratos inteligentes, ainda que o detalhamento normativo varie entre as experiências normativas estudadas. Na Ale-

manha, o reconhecimento jurídico dos contratos digitais decorre dos princípios gerais do Código Civil (BGB) e das normas europeias (eIDAS), baseando-se na autonomia privada, boa-fé e equivalência funcional, mas ainda sem disciplina técnica específica para contratos inteligentes. Nos EUA, legislações estaduais, como Arizona e Nevada, reconhecem a validade jurídica dos contratos inteligentes e do uso de blockchain, com forte ênfase na neutralidade tecnológica, mas sem o nível de detalhamento técnico do PL 4/2025. Na União Europeia, o *EU Data Act* e os princípios do *European Law Institute* começam a incorporar requisitos técnicos similares ao projeto brasileiro, sobretudo em termos de segurança, término seguro e auditabilidade dos contratos inteligentes. O Reino Unido e as normas da UNCITRAL também reconhecem contratos digitais e inteligentes, mas, em geral, ainda com foco em princípios contratuais tradicionais e na neutralidade tecnológica, sem o detalhamento normativo apresentado pelo PL 4/2025.

Os estudos de casos trataram especificamente dos contratos inteligentes, nos Estados Unidos, no Reino Unido e em Singapura, demonstrando os desafios sobre segurança, embora a tecnologia *blockchain* e dos *smart contracts* representem avanços importantes nesse sentido.

O capítulo dedicado aos contratos celebrados por meios digitais no PL 4/2025 reconhece a validade jurídica dos contratos digitais e incorpora conceitos fundamentais como imaterialidade, equivalência funcional e segurança jurídica. Desta forma, o legislador assegura que os contratos digitais tenham a mesma força normativa dos contratos tradicionais, desde que respeitados os requisitos legais de validade. A proposta inova ao regulamentar os *smart contracts*, por meio da previsão de requisitos mínimos de segurança, auditabilidade e controle de execução e ao disciplinar a validade dos contratos firmados por aplicativos digitais.

Assinaturas eletrônicas

As assinaturas eletrônicas desempenham um papel indispensável para celebração de contratos digitais, por meio de recursos como a criptografia e certificados digitais.

No cenário internacional, a UNCITRAL, já desde 2001, estabeleceu as bases normativas com a *Model Law on Electronic Signatures*, difundindo os princípios de equivalência funcional, neutralidade tecnológica e reconhecimento jurídico das assinaturas eletrônicas. Na União Europeia, o Regulamento eIDAS (910/2014) serve como principal referência. Assim como o PL 4/2025, o eIDAS distingue três níveis de assinatura: simples, avançada e qualificada.

A análise dos casos REsp 1.495.920 e REsp 2.022.423/RS demonstra a evolução e os desafios da aceitação das assinaturas eletrônicas e dos meios digitais de comunicação no direito contratual brasileiro. O primeiro julgado reforça a segurança jurídica conferida aos contratos eletrônicos assinados digitalmente, mesmo sem a presença de testemunhas, desde que garantida a integridade e autenticidade por meio de certificação eletrônica. Já o segundo caso evidencia as limitações do uso de e-mails como prova de comunicação em procedimentos que exigem notificação formal e inequívoca, como a constituição em mora em ações de busca e apreensão.

O tratamento normativo das assinaturas eletrônicas no Brasil se deu por meio da Medida Pro-

visória nº 2.200-2/2001, ao instituir a ICP-Brasil, e foi o primeiro marco regulatório, conferindo validade jurídica às assinaturas eletrônicas qualificadas mediante o uso de certificados digitais emitidos por autoridades certificadoras credenciadas. A ampliação do escopo normativo sobre assinaturas eletrônicas se deu pela a Lei nº 14.063/2020, responsável pela classificação das assinaturas eletrônicas em simples, avançadas e qualificadas, permitindo maior flexibilidade na escolha da modalidade conforme o nível de risco da operação e a exigência de segurança.

O Projeto de Lei nº 4, de 2025, consolida e atualiza o regime jurídico das assinaturas eletrônicas no Brasil, incorporando no Código Civil a disciplina expressa da matéria, a partir do reconhecimento da classificação trinária de assinaturas (simples, avançada e qualificada).

Em suma, o Projeto de Lei nº 4, de 2025, avança de forma sistemática e consistente no enfrentamento dos desafios trazidos pela digitalização das relações privadas, preenchendo lacunas normativas e introduzindo conceitos inéditos no ordenamento jurídico brasileiro, de forma articulada com os entendimentos jurisprudenciais dos tribunais superiores brasileiros, e tendências legislativas internacionais. A partir da análise detalhada dos capítulos que compõem o Livro de Direito Civil Digital, observa-se a preocupação do legislador em promover uma normatização que seja, ao mesmo tempo, principiológica e operacional. A inclusão do Livro Direito Civil Digital no Código Civil configura uma inovação legislativa sem precedentes entre os sistemas jurídicos analisados nesta pesquisa, demonstrando um esforço pioneiro de adaptação estrutural do direito privado aos desafios da era digital e reafirmando o compromisso com a proteção dos direitos fundamentais em um ambiente marcado pela crescente digitalização.

REFERÊNCIAS

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL. *Diretrizes para a Indústria sobre proteção infantil on-line. Publicações ITU*. Setor de Desenvolvimento da União Internacional de Telecomunicações. 2020. Disponível em: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/ec381712a6df3eacda178a4d62d17e9e. Acesso em: 20 out. 2024.

ALEMANHA. *Bürgerliches Gesetzbuch (BGB) — Código Civil Alemão*. Promulgado em 18 agosto 1896. Disponível em: https://www.gesetze-im-internet.de/bgb/. Acesso em: 15 jul. 2025.

ALEMANHA. *LG Berlim 20 (Zivilkammer). Aktenzeichen 20 O 172/15*. Berlim, 17 dez. 2015. Disponível em: http://www.Berlim.de/gerichte/presse/pressemitteilungen-der--ordentlichen-gerichtsbarkeit/2017/presse mitteilung.596076.php. Acesso em: 10 abr. 2025.

ALEMANHA. *Der Bundesgerichtshof (BGH). III ZR 183/17. Karlsruhe*, 12 jul. 2018. Disponível em: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=866 02&pos=0&anz=1. Acesso em: 10 abr. 2025.

ANDRIGHI, Nancy. *Herança digital: acesso e transmissibilidade post mortem de bens.* Salvador: Juspodium, 2025.

ANGELO, Tiago. Barroso considera Marco Civil insuficiente e propõe dois modelos de responsabilização das redes *Consultor Jurídico (ConJur)*, 18 dez. 2024. Disponível em: https://www.conjur.com.br/2024-dez-18/barroso-considera-marco-civil-insuficiente-e-propoe-dois-modelos-de-responsabilizacao-das-redes/. Acesso em: 16 jun. 2025.

APPLE. *Como adicionar um contato de legado à conta Apple.(2025a)* Disponível em: https://support.apple.com/pt-br/102631. Acesso em: 20 abr. 2025.

APPLE. *Termos e condições do iCloud*.(2025b). Disponível em: https://www.apple.com/ br/legal/internet-services/icloud/br/terms.html. Acesso em: 20 abr. 2025.

ARGENTINA. *Ley nº 25.326. Protección de los datos personales*. Buenos Aires: Boletín Oficial de la República Argentina, 04 oct. 2000. Disponível em: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acesso em: 29 maio 2025.

AUSTRÁLIA. *Criminal Code Amendment (Deepfake Sexual Material) Act 2024*. Canberra: Parlamento da Austrália, 2024. Disponível em: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7205. Acesso em: 24 jun. 2025.

AZEVEDO, Álvaro Villaça. *Curso de Direito Civil: Teoria Geral dos Contratos*. 4. Ed. São Paulo: Saraiva Educação, 2019.

BARROSO, Luís Roberto; BARROSO, Luna Van Brussel. Democracia, mídias sociais e liberdade de expressão: ódio, mentiras e a busca da verdade possível. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 17, n. 49, p. 285-311, jul./dez. 2023, p.291-293.

BEIDACKI, C.; FARIAS, B.; BENATTI, G.; BOEIRA, L. *Tempo de tela para crianças e adolescentes: respostas rápidas para governos – evidências, desafios e caminhos possíveis*. São Paulo: Instituto Veredas, 2024. Disponível em: https://www.veredas.org/wordpveredas/wp-content/uploads/2024/07/OK-VOL-2_Veredas_Respostas-Rapidas_Final2-1.pdf. Acesso em: 20 maio 2025.

BERNARD, Tim. *144 state bills aim to secure child online safety as Congress flounders*. Tech Policy Press, 22 maio 2023. Disponível em: https://techpolicy.press/144-state-bills-aim-to-secure-child-online-safety-as-congress-flounders/. Acesso em: 26 jun. 2025.

BIK, T. *B. I. for K. The Better Internet for Kids (BIK)*. 2021. Disponível em: https://www.betterinternetforkids.eu/en-GB/. Acesso em: 22 nov. 2024.

BIONI, Bruno Ricardo; LISBOA, Roberto Senise. A formação e a conclusão dos contratos eletrônicos. *In: Revista FMU Direito*. São Paulo, ano 24, n. 32, 2010.

BORELLI, Alessandra. *Crianças e adolescentes no mundo digital: Orientações essenciais para o uso seguro e consciente das novas tecnologias*. São Paulo: Autêntica Editora, 2022.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735. Acesso em: 10 abr. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 3.050, de 2020*. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1997738. Acesso em: 20 abr. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 410, de 2021*. Acrescenta artigo à Lei do Marco Civil da Internet – Lei no 12.965, de 23 de abril de 2014, a fim de dispor sobre a destinação das contas de internet após a morte de seu titular. Brasília:

Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2270016. Acesso em: 20 abr. 2025.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 1.144, de 2021. Dispõe sobre os dados pessoais inseridos na internet após a morte do usuário. Brasília, DF, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2275941. Acesso em: 15 jul. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.664, de 2021*. Acrescenta o art. 1857-A à Lei n° 10406, de 2002, Código Civil, de modo a dispor sobre a herança digital.Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2061744&filename=Avulso%20PL%202664/2021. Acesso em: 20 abr. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 365, de 2022*. Dispõe sobre a herança digital. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151903. Acesso em: 20 abr. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 703, de 2022.* Acrescenta o art. 1857-A à Lei n° 10406, de 2002, Código Civil. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2318667. Acesso em: 20 abr. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 954, de 2022*. Altera a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), para dispor sobre contratos automatizados (smart contracts). Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/propostas-legislativas/2320041. Acesso em: 18 jun. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.174, de 2023*. Estabelece as normas e princípios para proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, objetivando garantir a proteção e promoção dos neurodireitos dos indivíduos. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2264479&filename=PL%202174/2023. Acesso em: 17 jun. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 4.691, de 4 de dezembro de 2024.* Dispõe sobre o direito e a garantia fundamental à livre manifestação do pensamento na Internet, a vedação ao anonimato, o exercício da atividade econômica em plataformas digitais, organização e funcionamento das plataformas, serviços e mercados digitais na Internet, e dá outras providências. Brasília, DF: Câmara dos Deputados, 2024. Disponível em:https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2475865. Acesso em: 17 jun. 2025.

BRASIL. Congresso Nacional. *Proposta de Emenda à Constituição nº 29, de 2023*. Altera a Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica. Brasília: Congresso Nacional, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095. Acesso em: 18 out. 2024.

BRASIL. Conselho Nacional de Autorregulamentação Publicitária (CONAR). *Representação nº 134/2023.* Julga procedimento instaurado contra publicidade considerada inadequada ou enganosa. Brasília: CONAR, 2023. Disponível em: http://www.conar.org.br/processos/detcaso.php?id=6354. Acesso em: 10 abr. 2025.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). *Resolução nº 163, de 13 de março de 2014.* Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Brasília: CONANDA, 2014. Disponível em: https://www.gov.br/mdh/pt-br/acesso-a-informacao/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda/resolucoes/resolucao-163-_publicidade-infantil.pdf/view. Acesso em: 10 abr. 2025.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). *Resolução nº 245, de 15 de fevereiro de 2024.* Dispõe sobre a proteção integral de crianças e adolescentes em ambientes digitais e estabelece diretrizes para a publicidade e a comunicação mercadológica dirigida a esse público. Brasília: CONANDA, 2024. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/48630. Acesso em: 10 abr. 2025.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 15 jul. 2025.

BRASIL. Estado do Rio Grande do Sul. Emenda Constitucional nº 85, de 2023. Disponível em: http://ww3.al.rs.gov.br/filerepository/repLegis/arquivos/EC%2089-85.pdf. Acesso em: 26 jun. 2025.

BRASIL. Estado de São Paulo. *Lei nº 12.730, de 11 de outubro de 2007*. Proíbe o uso telefone celular nos estabelecimentos de ensino do Estado, durante o horário de aula. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2007.Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/2007/lei-12730-11.10.2007.html. Acesso em: 26 jun. 2025.

BRASIL. Estado de São Paulo. *Lei nº 18.058, de 5 de dezembro de 2024*. Altera os artigos 1º a 3º e inclui artigos 4º a 6º na Lei nº 12.730/2007, proibindo a utilização de celulares e outros dispositivos eletrônicos pelos alunos nas unidades escolares da rede pública e privada de ensino. Diário Oficial do Estado de São Paulo, São Paulo, 6 dez. 2024. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/2024/lei-18058-05.12.2024.html. Acesso em: 26 jun. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor*. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 17 jun. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 jun. 2025.

BRASIL. *Lei nº 13.105*, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União: seção 1, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 17 jun. 2025.

BRASIL. *Lei nº 13.185, de 6 de novembro de 2015*. Institui o Programa de Combate à Intimidação Sistemática (bullying) em todo o território nacional. Diário Oficial da União: seção 1, Brasília, DF, 9 nov. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 26 jun. 2025.

BRASIL. *Lei nº 13.257, de 8 de março de 2016*. Dispõe sobre políticas públicas para a primeira infância e altera as Leis nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), nº 8.742, de 7 de dezembro de 1993 (Lei Orgânica da Assistência Social), nº 11.770, de 9 de setembro de 2008, e nº 12.662, de 5 de junho de 2012. Diário Oficial da União: seção 1, Brasília, DF, 9 mar. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13257.htm. Acesso em: 18 out. 2024.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 out. 2024.

BRASIL. *Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001*. Diário Oficial da União: seção 1, Brasília, DF, 24 set. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso em: 18 out. 2024.

BRASIL. *Lei nº 15.100, de 13 de janeiro de 2025*. Dispõe sobre a utilização, por estudantes, de aparelhos eletrônicos portáteis pessoais nos estabelecimentos públicos e privados de ensino da educação básica. Diário Oficial da União: Seção 1, Brasília, DF, 14 jan. 2025. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2025/lei-15100-13-janeiro-2025-796892-publicacaooriginal-174094-pl.html.Acesso em: 18 out. 2024.

BRASIL. *Lei nº 15.123, de 24 de abril de 2025*. Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer medidas relacionadas à proteção de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 25 abr. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em: 24 jun. 2025.

BRASIL. *Medida Provisória nº 2.200-2, de 24 de agosto de 2001*. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 27 ago. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 18 out. 2024.

BRASIL. Ministério Público do Estado do Rio de Janeiro. *Procedimento Preparatório nº 1.30.001.001561/2016-05*. Rio de Janeiro, RJ: MPRJ, 2016.

BRASIL. Secretaria de Comunicação Social da Presidência da República. *Crianças, adolescentes e telas: guia sobre usos de dispositivos digitais [li*vro eletrônico]. Brasília, DF: Secretaria de Comunicação Social da Presidência da República, 2024. p. 15–16. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 25 maio 2025.

BRASIL. Senado Federal. *Parecer nº 1 – Subcomissão de Direito Digital da CJCOD-CIVIL.* Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/34470bd2-bc45-4144-aa1c-7941d5488c0d. Acesso em: 15 jul. 2025.

BRASIL. Senado Federal. *Projeto de Lei nº 5.820, de 2019.* Brasília, DF: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/153680. Acesso em: 20 abr. 2025.

BRASIL. Senado Federal. *Projeto de Lei nº 6.468, de 2019*. Altera o Código Civil para determinar a transmissão aos herdeiros de todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança. Brasília, DF: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140239. Acesso em: 20 abr. 2025.

BRASIL. Senado Federal. *Projeto de Lei nº 1.229, de 2021*. Modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção. Brasília, DF: Senado Federal, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2276604&fichaAmigavel=nao. Acesso em: 18 out. 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 522, de 2022*. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para conceituar "dado neural" e regulamentar sua proteção. Brasília, DF: Senado Federal, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524. Acesso em: 18 out. 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 2.338, de 2022. Dispõe sobre o uso da Inteligência Artificial.* Brasília, DF: Senado Federal, 2022. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 18 out. 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 4.691, de 2024*. Dispõe sobre o direito e a garantia fundamental à livre manifestação do pensamento na internet, os termos da vedação ao anonimato na internet, o livre exercício da atividade econômica na internet, a organização e funcionamento das plataformas, serviços e mercados digitais na internet e dá outras providências. Brasília, DF: Senado Federal, 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2475865#:~:text=Dispõe%20sobre%20o%20direito%20e,internet%20e%20dá%20outras%20providências. Acesso em: 18 out. 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 145, de 2024.* Altera o Código de Defesa do Consumidor (Lei nº 8.078, de 1990) para regular o uso de inteligência artificial em publicidade e coibir a publicidade enganosa com o uso dessas ferramentas. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/161946. Acesso em: 24 jun. 2025.

BRASIL. Senado Federal. *Projeto de Lei nº 146, de 2024*. Altera o Código Penal (Decreto-Lei nº 2.848, de 1940) para agravar a pena em crimes contra a honra ou falsa identidade praticados com uso de inteligência artificial. Brasília, DF: Senado Federal, 2024. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/161947. Acesso em: 24 jun. 2025.

BRASIL. Senado Federal. Proposta de Emenda à Constituição nº 29, de 13 de junho de 2023. Altera a Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095. Acesso em: 15 jul. 2025.

BRASIL. Minas Gerais. Tribunal Regional Eleitoral. *Mandado de Segurança nº 0600808-47.2024.6.13.0000,* Rel. Juíza Flávia Birchal, julgado em 22 ago. 2024. Disponível em: https://consultaunificadapje.tse.jus.br/consulta-publica-unificada/documento?extensaoArquivo=text/html&path=regional/mg/2024/9/10/21/11/46/b949ec18da56bc3cdf0e478688fa3b068a5d877d50ccb92d4585f127a3e8d649. Acesso em: 15 jul. 2025.

BRASIL. Pernambuco. Tribunal Regional Eleitoral. *Recurso Eleitoral nº 06000741 3.2024.6.17.0121*, Rel. Des. Filipe Fernandes Campos, julgado em 8 ago. 2024. Disponível em: https://consultaunificadapje.tse.jus.br/consulta-publica-unificada/documento?extensaoArquivo=text/html&path=regional/pe/2024/8/8/12/38/5/. Acesso em: 15 jul. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.334.097/RJ*. Rel. Min. Luis Felipe Salomão, julgado em 28 maio 2013.(2013a) Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=31006510&tipo=0&nreg=&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=&formato=PDF&salvar=false. Acesso em: 25 maio 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.335.153/RJ*. Rel. Min. Luis Felipe Salomão, julgado em 28 maio 2013. (2013b) Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=31006938&tipo=0&nreg=&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=&formato=PDF&salvar=false. Acesso em: 25 maio 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.444.008/RS*. Rel. Min. Nancy Andrighi, julgado em 25 out. 2016. Diário da Justiça Eletrônico, Brasília, DF, 9 nov. 2016. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=66541484&tipo=5&nreg=201400646460&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20161109&formato=PDF&salvar=false. Acesso em: 13 jun. 2025.

BRASIL. Superior Tribunal de Justiça. *Agravo interno no Recurso Especial nº 1.593.873/SP (2016/0079618-1).* Rel. Min. Nancy Andrighi, julgado em 10 nov. 2016. Diário da Justiça Eletrônico, Brasília, DF, 17 nov. 2016. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=66956727&tipo=0&nreg=&S. Acesso em: 13 jun. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.634.851/RJ.* Rel. Min. Nancy Andrighi, julgado em 12 set. 2017. Brasília, DF: STJ, 2018. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?CodOrgaoJgdr=&SeqCgrmaSessao=&dt=20180215&formato=PDF&nreg=201502262739&salvar=false&seq=1576048&tipo=0 . Acesso em: 13 jun. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.660.168/RJ*. Rel. Min. Nancy Andrighi, julgado em 8 maio 2018. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=83459361&tipo=0. Acesso em: 13 jun. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.495.920/DF*. Rel. Min. Paulo de Tarso Sanseverino, Terceira Turma, julgado em 15 maio 2018. Diário de Justiça Eletrônico, 7 jun. 2018. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?CodOrgaoJgdr=&SeqCgrmaSessao=&dt=20180607&formato=PDF&nreg=20140295+3009&salvar=false&seq=78697795&tipo=5. Acesso em: 10 abr. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 2.022.423/RS*. Rel. Min. Nancy Andrighi, julgado em 25 abr. 2023. Brasília, DF: STJ. Disponível em: https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?CodOrgaoJgdr=&SeqCgrmaSessao=&dt=20230427&formato=PDF&nreg=202202664680&salvar=false&seq=228945 1&tipo=0 . Acesso em: 13 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Guia ilustrado contra as deepfakes*. Brasília, DF: Supremo Tribunal Federal; Data Privacy Brasil, Coordenadoria de Combate à Desinformação, 2024. Disponível em: https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf Acesso em: 10 abr. 2025.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário RE 1.037.396/SP – Tema 987 da Repercussão Geral.* (2025a). Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987. Acesso em: 16 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 1.057.258/MG* – Tema 533 (Repercussão Geral). Rel. Min. Luiz Fux, julgado em 27 nov. 2024. Brasília, DF: STF, 2024. Disponível em: https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/06/11212526/RE-1057258-Voto-LF.pdf. Acesso em: 13 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Tema 533 da Repercussão Geral: possibilidade de responsabilização objetiva do provedor de aplicação de internet por conteúdo gerado por terceiros*. Brasília, DF: STF, (2025b). Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=533. Acesso em: 16 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Tema 786 da Repercussão Geral: responsabilidade civil do provedor de internet por atos ilícitos praticados por terceiros*. Brasília, DF: STF, 2021. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. Acesso em: 5 abr. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade (ADI) nº 5.631–BA*. Rel. Min. Edson Fachin, julgado em 25 mar. 2021. Brasília, DF: STF, 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/1218978035/inteiro-teor-1218978037. Acesso em: 16 jul. 2025.

BRASIL . Supremo Tribunal Federal. *Recurso extraordinário nº 1.010.606 (Tema 786 – repercussão geral).* Relator: Min. Dias Toffoli. Julgamento em 11 fev. 2021. Dispo-

nível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. Acesso em: 30 jun. 2025.

BRASIL. Supremo Tribunal Federal *STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros*. Brasília: STF, 26 jun. 2025. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/. Acesso em: 26 jun. 2025.

BRASIL. Tribunal de Justiça de Minas Gerais (3ª. Câmara Cível). *Agravo de Instrumento 1.0000.21.190675-5/001*. AGRAVO [...] Recurso conhecido, mas não provido. Agravante: Josilene Menezes Folgado. Agravado: Alexandre Lana Ziviani. Relatora: Albergaria Costa. Minas Gerais, 28 de janeiro de 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-mg/1363160167/inteiro-teor-1363160241. Acesso em: 20 abr. 2025.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais (8ª Câmara Cível Especializada). *Agravo de Instrumento 1743814-30.2024.8.13.0000*. Agravante: Orlando De Oliveira Vaz Neto Espólio De, Repdo P/ Invte José Otávio De Vianna Vaz. Interessado: Maria Isabel Vianna De Oliveira Vaz, Orlando De Oliveira Vaz Filho. Relator: Des.(a) Delvan Barcelos Júnior. Belo Horizonte, 22 de maio de 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-mg/2581235540. Acesso em: 20 abr. 2025.

BRASIL. Tribunal de Justiça do Estado da Paraíba (3ª Câmara Cível). *Agravo de Instrumento 0808478-38.2021.8.15.0000*. AGRAVO INTERNO [...] DECISÃO QUE NÃO CAUSA PREJUÍZO À EMPRESA. MANUTENÇÃO, DESPROVIMENTO DO AGRAVO INTERNO. Agravante: Geraldo Jose Barral Lima. Agravado: Facebook Serviços Online do Brasil Ltda. Relator: Marcos Cavalcanti de Albuquerque. Paraíba, 28 de fevereiro de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pb/1774059642 Acesso em: 10 abr. 2025.

BRASIL. Tribunal de Justiça do Estado de São Paulo (27ª Câmara de Direito Privado). *Apelação 1123920-82.2023.8.26.0100*. Apelante: Ivanilsa Rodrigues Dos Santos. Apelado: Facebook Serviços Online Do Brasil Ltda. e Google Brasil Internet Ltda. Relator: Celina Dietrich Trigueiros. Jacareí, 30 de agosto de 2024. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=18288395&cdForo=0. Acesso em: 10 abr. 2025.

BRASIL. Tribunal Superior Eleitoral. *Resolução nº 23.732, de 27 de fevereiro de 2024*. Altera a Resolução-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. *Diário da Justiça Eletrônico do TSE*, Brasília, DF, n. 29, p. 132–145, 4 mar. 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 24 jun. 2025.

BURILLE, C.; HONORATO, G.; LEAL, L. T. Danos morais por exclusão de perfil de pessoa falecida? Comentários ao acórdão proferido na apelação cível n. 1119688-66.2019.8.26.0100 (TJSP). *Revista Brasileira de Direito Civil* – RBDCivil, Belo Horizonte, v. 28, abr./jun. 2021. p. 212-229.

CANELLO, Júlio. Os Contratos Eletrônicos no Direito Brasileiro: comentários sobre o tempo e lugar da formação contratual. *In: Revista Sociais e Humanas*, v. 20, n. 01, jan/jun 2007. p. 9-22.

CASTELLO, Juliana Justo Botelho. Tiktok ban, constitucionalismo digital e jurisdição: opacidade do legal design e esvaziamento dos dados. *Migalhas* de Peso, 11 maio 2023. Disponível em: https://www.migalhas.com.br/depeso/386354/tiktok-ban--constitucionalismo-digital-e-jurisdicao. Acesso em: 22 nov. 2024.

CASTELLS, Manuel. *A sociedade em rede,* 6. ed. São Paulo: Paz e Terra, 2018.

CASTRO, C. A.; CARTHY, A.; O'REILLY, I. An ethical discussion about the responsibility for protection of minors in the digital environment: a state-of-the-art review. *Advances in Social Sciences Research Journal*, v. 9, n. 5, p. 343-370, 2022.

CHILE. Ley nº 19.628. Sobre protección de la vida privada. Santiago: Biblioteca del Congreso Nacional de Chile, 28 ago. 1999. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=141599. Acesso em: 29 maio 2025.

CHILE. Ley nº 21.383, de 14 de octubre de 2021. Modifica la Constitución Política para establecer que "el desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica». Diario Oficial de la República de Chile, Santiago, 25 oct. 2021. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1166983. Acesso em: 16 jul.2025.

CHILE, Corte Constitucional, processo nº 105.065-2023, relatora Ministra Ángela Vivanco, j. em 9/8/2023. Disponível em: https://www.doe.cl/alerta/11082023/20230811001. Acesso em: 2 dez. 2024.

CHILE. *Constitución política de la República de Chile*. Capitulo III de los derechos y deberes constitucionales. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 18 out 2024.

CHINA. *Regulamento sobre a Gestão de Serviços de Informação na Internet com Síntese Profunda*. Promulgado em 12 dez. 2022. Disponível em: https://www-china--briefing-com.translate.goog/news/china-to-regulate-deep-synthesis-deep-fake--technology-starting-january-2023/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 24 jun. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024. São Paulo: CGI.br, 2024. Disponível em: https://cetic.br/pt/pesquisa/kids-online/indicadores/. Acesso em: 15 jul. 2025.

CRIANÇA E CONSUMO. Youtubers mirins. (2016). Disponível em: https://criancaeconsumo.org.br/nossa-atuacao/atuacao-juridica/acoes-juridicas/youtubers-mirins/. Acesso em: 10 nov. 2024.

CRIANÇA E CONSUMO. Mattel do Brasil LTDA. Você Youtuber Escola Monster High. (2017). Disponível em: https://criancaeconsumo.org.br/nossa-atuacao/atuacao-juridica/acoes-juridicas/mattel-do-brasil-ltda-voce-youtuber-escola-monster-high-fevereiro2017/ Acesso em: 10 nov. 2024.

DAVENPORT, Thomas H; BECK, John C. *Economia da atenção*. Rio de Janeiro: Elsevier, 2001.

DE LUCCA, Newton. Direito do consumidor. São Paulo: Quartier Latin, 2003.

DOMO. *Data Never Sleeps 12.0: infographic. 12º Relatório "Data Never Sleeps"*. Disponível em: https://www.domo.com/learn/infographic/data-never-sleeps-12?utm_source=wire&utm_medium=pr&utm_campaign=PR_Domo_Data_Never_Sleeps_12&-campid=701Vq000001ztWzIAI. Acesso em: 15 jul. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados*. São Paulo: Thomson Reuters Brasil, 2021.

ESPANHA. *Carta de Derechos Digitales*. Aprovada em 14 de julho de 2021. Disponível em: https://www.derechosdigitales.gob.es/es/carta-espanola-de-derechos-digitales. Acesso em: 18 out 2024.

ESPANHA. *Estrategia Nacional de Ciberseguridad 2019*. Madrid: Departamento de Seguridad Nacional (DSN), Consejo de Seguridad Nacional, 26 abr. 2019. Disponível em: https://www.dsn.gob.es/sites/default/files/documents/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf. Acesso em: 24 jun. 2025.

ESPANHA. *Ley Orgánica 1/1996,* de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. *Boletín Oficial del Estado*, n. 15, p. 1225–1238, 17 jan. 1996. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1996-1069. Acesso em: 24 jun. 2025.

ESPANHA. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. "Boletín Oficial del Estado" (España), n° 294, de 6 diciembre 2018, pp. 119 788–119 857. Referência BOEA201816673. Promulgada em 5 dez. 2018. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673. Acesso em: 17 jun. 2025.

ESTADOS UNIDOS. Arizona. *Arizona Revised Statutes*, tit. 44, § 44 7061, de 2024 — Signatures and records secured through blockchain technology; smart contracts; ownership of information; definitions. Disponível em: https://law.justia.com/codes/arizona/title-44/section-44-7061/. Acesso em: 24 jun. 2025.

ESTADOS UNIDOS DA AMÉRICA. *Arizona Electronic Transactions Act (AETA),* Arizona Revised Statutes, Title 44, Chapter 26. Phoenix: State of Arizona, 2000. Disponível em: https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/44/07001.htm. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Clayton Antitrust Act*, 15 de outubro de 1914. Disponível em: https://www.ftc.gov/legal-library/browse/statutes/clayton-act. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. *California Consumer Privacy Act (CCPA)*, California Civil Code §§ 1798.100 – 1798.199. Sacramento: State of California, 2020. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. California. House of Legislative. *Protecting Our Kids from Social Media Addiction Act* (SB 976). Disponível em: https://digitaldemocracy.calmatters.org/bills/ca_202320240sb976. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Communications Decency Act (CDA),* 1996. Disponível em: https://uk.practicallaw.thomsonreuters.com/9-502-8947?transitionType=Default&contextData=(sc.Default)&firstPage=true. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS. *Commodity Futures Trading Commission v. My Big Coin Pay, Inc., No. 1:18-cv-10077,* U.S. District Court for the District of Massachusetts, julgamento em 26 set. 2018. Disponível em: https://www.cftc.gov/sites/default/files/2018-10/enfmybigcoinpayincmemorandum092618.pdf. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Deceptive Consumer Sales Act de Indiana*, 1971. Disponível em: https://law.justia.com/codes/indiana/title-24/article-5/chapter-0-5/. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS. *Digital Millennium Copyright Act of 1998: DMCA*. Public Law nº 105-304, 28 oct. 1998. Disponível em: https://www.copyright.gov/legislation/dmca.pdf. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Electronic Signatures in Global and National Commerce Act (E-Sign Act)*, Pub. L. No. 106-229, 114 Stat. 464, 30 June 2000. Codificado em 15 U.S.C. §§ 7001–7031. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Federal Trade Commission Act,* 26 de setembro de 1914. Disponível em: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS. *Filter Bubble Transparency Act*, 2024. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/2024/text. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Protecting Americans from Foreign Adversary Controlled Applications Act (H.R. 7521).* Public Law nº 118-50, aprovado em 24 abr. 2024. Disponível em: https://www.congress.gov/bill/118th-congress/house-bill/7521/text. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. *Federal Trade Commission (FTC). In the Matter of Meta Platforms,* Inc.; Mark Zuckerberg; and Within Unlimited, Inc. Matter/File Nº 221 0040; Docket Nº 9411. Administrative Proceeding. Caso encerrado em 24 de fevereiro de 2023. Disponível em: https://www.ftc.gov/legal-library/browse/cases-proceedings/221-0040-metazuckerbergwithin-matter. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. SUPREME COURT. *Gonzalez v. Google LLC, 596* U.S. ___ (2023). Disponível em: https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *H.R.7766 - Protecting Consumers from Deceptive AI Act.* Disponível em: https://www.congress.gov/bill/118th-congress/house-bill/7766/text/ih. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Children and Teens' Online Privacy Protection Act HR 7890* (2018). Disponível em: https://d1dth6e84htgma.cloudfront.net/H_R_7890_Children_and_Teens_Online_Privacy_Protection_Act_Walberg_96cfcb8745.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Children's Online Privacy Protection Act (COPPA),* 15 U.S. Code §§ 6501–6506. Washington, D.C.: United States Congress, 1998. Disponível em: https://www.law.cornell.edu/uscode/text/15/chapter-91. Acesso em: 29 maio 2025.

ESTADOS UNIDOS DA AMÉRICA. *Kids Online Safety Act HR7891*. Disponível em: https://d1dth6e84htgma.cloudfront.net/H_R_7891_Kids_Online_Safety_Act_0f114319bc.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Kids Online Safety and Privacy Act – KOSPA.* Disponível em: https://cdn.sanity.io/files/3tzzh18d/production/c6acc4e435eba7dfeb620c2457a69818d28961d9.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Minnesota Age-Appropriate Design Code Act*. Disponível em: https://www.house.mn.gov/comm/docs/2hlcmA4QN0K9KVMGRvzBpw.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *NetChoice v. Bonta*. Disponível em: https://cdn.sanity.io/files/3tzzh18d/production/9e19c8974ba93d881c6b8629801d0bab7aea18ce.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. Nevada. *Nevada Revised Statutes, Chapter 719, § 719.240. Electronic Records and Signatures; Use of Blockchain Technology and Smart Contracts.* Carson City: State of Nevada, 2017. Disponível em: https://www.leg.state.nv.us/NRS/NRS-719.html#NRS719Sec240. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. New York. House of Legislative. *Stop Addictive Feeds Exploitation (SAFE) for Kids Act (HB7694).* Disponível em: https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Sherman Antitrust Act*, 2 de julho de 1890. Disponível em: https://www.archives.gov/milestone-documents/sherman-anti-trust-act. Acesso em: 15 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. *Twitter, Inc. v. Taamneh, 598 U.S. 471* (2023). Julgado em 18 de maio de 2023. Disponível em: https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS. SUPREME COURT OF THE UNITED STATES OF AMERICA (SCOTUS). *Moody v. NetChoice, LLC*. Disponível em: https://www.supremecourt.gov/docket/docketfiles/html/public/22-277.html. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS. SUPREME COURT OF THE UNITED STATES OF AMERICA (SCOTUS). *NetChoice, LLC, DBA NetChoice, et al. v. Ken Paxton, Attorney General of Texas*. [31 maio 2022]. Disponível em: https://www.supremecourt.gov/opinions/23pdf/22-277new_8mjp.pdf. Acesso em: 22 nov. 2024.

ESTADOS UNIDOS. Tennessee. *Tennessee Code, Title 47, Chapter 10, Part 2, Section 4710201 (2024)*. Disponível em: https://law.justia.com/codes/tennessee/title-47/chapter-10/part-2/section-47-10-201/. Acesso em: 26 jun. 2025.

EUROPEAN LAW INSTITUTE. *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*. Viena: European Law Institute, 2022. ISBN 978-3-9505192-9-7. Disponível em: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf. Acesso em: 24 jun. 2025.

FACEBOOK. *Como administrar a conta de uma pessoa falecida*. 2025. Disponível em: https://www.facebook.com/help/275013292838654/ ?helpref=hc_fnav. Acesso em: 20 abr. 2025.

FLORIDI, Luciano. *The onlife manifesto: being a human in a hiperconnected era.* Springer, 2014.

FLORIDI, Luciano. *The Right to be Forgotten: A Philosophical View*. 2015. Disponível em: https://ssrn.com/abstract=3853478. Acesso em: 13 jun. 2025.

FOGG, B. J. *Persuasive technology: using computers to change what we think and do (interactive technologies).* Morgan Kaufmann, 2002.

FRANÇA. *Charte de Développement Responsable des Neurotechnologies*. Ministère chargé de l'Enseignement supérieur et de la Recherche, 17 nov. 2022. Disponível em: https://www.enseignementsup-recherche.gouv.fr/fr/charte-de-developpement--responsable-des-neurotechnologies-87964. Acesso em: 15 jul. 2025.

FRITZ, Karina Nunes. Leading Case: BGH reconhece a transmissibilidade da herança digital. *German Report – Migalhas*, São Paulo, 13 de agosto de 2019. Atualizado às 07:44. Disponível em: https://www.migalhas.com.br/coluna/german-report/308578/leading-case--bgh-reconhece-a-transmissibilidade-da-heranca-digital. Acesso em: 17 jun. 2025.

G1. *Implantação de chip cerebral da 'Neuralink', de Elon Musk, divide opiniões de especialistas; veja como funciona*. Disponível em: https://g1.globo.com/fantastico/noticia/2024/02/04/implantacao-de-chip-cerebral-da-neuralink-de-elon-musk-divide-opinioes-de-especialistas-veja-como-funciona.ghtml. Acesso em: 02 out. 2024.

GILLESPIE, Tarleton. The politics of 'platforms'. *New Media & Society*. V. 12. N. 3, p. 347-364, 2010.

GOBBO, Leandro Oliveira. *Smart contracts e o direito contratual brasileiro*. Tese (Doutorado em Direito Constitucional). Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), 2022. Disponível em: https://repositorio.idp.edu.br//handle/123456789/4652. Acesso em: 24 jun 2025.

GOOGLE. *Política de uso proibido da IA generativa*. 17 dez. 2024. (2024a). Disponível em: https://policies.google.com/terms/generative-ai/use-policy?hl=pt-BR. Acesso em: 24 jun. 2025.

GOOGLE. *Remover informações pessoais dos resultados da pesquisa*. Google Suporte, 2024. (2024b) Disponível em: https://support.google.com/websearch/troubleshooter/9685456. Acesso em: 01 jun. 2025

GOOGLE; IPSOS. *Our life with AI: from innovation to application* [livro eletrônico]. Janeiro de 2025. Disponível em: https://static.googleusercontent.com/media/publicpolicy.google/en//resources/ipsos_google_our-life-with-ai_2024_25.pdf. Acesso em: 24 jun. 2025.

GOOGLE. *Enviar uma solicitação a respeito da conta de um usuário falecido*. 2025. Disponível em: https://support.google.com/accounts/troubleshooter/6357590?hl=pt-BR Acesso em: 5 abr. 2025.

GUARDIA, A. F. T. S. Brevíssima incursão jurisprudencial – direito ao esquecimento e rompimento de vínculo entre o nome e o resultado de busca na internet. *Revista Internacional Consinter de Direito*, Paraná, Brasil, v. 6, n. 10, p. 59–79, 2020. Disponível em: https://revistaconsinter.com/index.php/ojs/article/view/135. Acesso em: 13 jun. 2025.

HABERLE, Peter. *Hermenêutica Constitucional, A sociedade aberta dos intérpretes da Constituição: Contribuição para a Interpretação Pluralista e 'Procedimental' da Constituição.* Tradução Gilmar Ferreira Mendes. Porto Alegre: Sergio Antônio Fabris, 1997.

HAN, Byung-Chul. *No enxame: perspectivas do digital*. Tradução de Lucas Machado. Petrópolis, RJ: Vozes, 2018.

IENCA, Marcello; ADORNO, Roberto. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sci Soc Policy* 13, 5 (2017). Disponível em: https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1. Acesso em: 4 out. 2024.

ÍNDIA. Supremo Tribunal. *Smt. Selvi & Ors. vs. State of Karnataka*, Apelação Criminal nº 1267 de 2004. Relator: Ministro J. Balakrishnan. Julgado em 05 de maio de 2010. Disponível em: https://api.sci.gov.in/jonew/judis/36303.pdf. Acesso em: 28 maio 2025.

INSTAGRAM. *Como denunciar a conta de uma pessoa falecida no Instagram*. 2025. Disponível em: https://help.instagram.com/264154560391256/. Acesso em: 20 abr. 2025.

INSTAGRAM. *Sobre as configurações de privacidade e segurança para adolescentes no Instagram*. Disponível em: https://help.instagram.com/3237561506542117. Acesso em: 24 jun. 2025.

IWF. *How AI is being abused to create child sexual abuse imagery*. Outubro, 2023. Disponível em: https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public--oct23v1.pdf. Acesso em 10 abr. 2025.

JUNQUILHO, Tainá Aguiar; SILVEIRA, Marilda de Paula; FERREIRA, Lucia Maria Teixeira; MENDES, Laura Schertel; OLIVEIRA, Andre Gualtieri de. (org.). *Construindo consensos: deep fakes nas eleições de 2024 relatório das decisões dos TREs sobre deep fakes.* Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa: Laborato- rio de Governança e Regulação de Inteligencia Artificial, 2024. Disponível em: https://www.idp.edu.br/arquivos/cedis/IDP%20-%20LIA%2C%20CEDIS%20e%20ETHICS4AI%20-%20Nota%20Técnica%20-%20Construindo%20Consensos%20-%20Deep%20Fakes%20nas%20Eleições%20de%202024.pdf. Acesso em: 24 jun. 2025.

LAZAI JUNIOR, Márcio; JUSTUS, Álvaro; LOURES, Eduardo Rocha; SANTOS, Eduardo Alves Portela; SZEJKA, Anderson Luis. Interoperability analysis in the functional machinery safety management in the automotive industry. *Brazilian Journal of Development*, v. 6, n. 1, p. 01–14, jan. 2020. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/6237/5534. Acesso em: 19 jun. 2025.

LEAL, Livia Teixeira. Tratamento jurídico do conteúdo disposto na internet após a morte do usuário e a denominada herança digital. In: TEIXEIRA, Daniele Chaves (Coord.). *Arquitetura do planejamento sucessório.* Belo Horizonte: Fórum, 2019.

LIMA, Aurea Andressa Lacerda. Uma visão geral sobre os neurodireitos. (2024a) *Migalhas,* 06/05/2024. Disponível em: https://www.migalhas.com.br/depeso/406643/uma-visao-geral-sobre-os-neurodireitos. Acesso em: 18 out. 2024

LIMA, Cintia Rosa Pereira de; SAMPAIO NETO, Walter Francisco. Smart contracts: desafios e perspectivas a partir da proposta no Projeto de Código Civil. *Migalhas*, 26/07/2024. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/412040/smart-contracts-desafios-a-partir-da-proposta-no-projeto-de-cc. Acesso em: 18 out. 2024

LUZ, Pedro Henrique Machado da; WACHOWICZ, Marcos. O "direito à desindexação": repercussões do caso González vs Google Espanha. *Espaço Jurídico Journal of Law [EJJL]*, v. 19, n. 2, p. 581–592, 2018. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/16492. Acesso em: 13 jun. 2025.

MARQUES, Cláudia Lima. *Comentários ao Código de Defesa do Consumidor*. 5. ed. São Paulo: RT, 2015.

MELLO, Marcos Bernardes de. *Teoria do fato jurídico: plano da existência*. 20 ed. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar-Revista de Ciências Jurídicas*, v. 25, n. 4, 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828. Acesso em: 24 maio 2025

MENDES, Laura Schertel Ferreira; FRITZ, Karina Nunes. Case Report: Corte Alemã Reconhece a Transmissibilidade da Herança Digital. *Direito Público*, [S. l.], v. 15, n. 85, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3383. Acesso em: 20 abr. 2025. p. 192.

META. Legal *Requests and Content Removal. Meta Transparency Center*, 2024a. Disponível em: https://transparency.meta.com/pt-br/ Acesso em: 1 jun. 2025.

META. *Denunciar conteúdo no Instagram.* Meta Help Center, 2024. Disponível em: https://help.instagram.com/535503073130320. Acesso em: 1 jun. 2025.

META. *Our Approach to Labeling AI-Generated Content and Manipulated Media.* 5 abr. 2024. Disponível em: https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/. Acesso em: 2 jun. 2025.

META. *Pedido de remoção legal. Meta*, 2025. Disponível em: https://www.facebook.com/help/874680996209917/?locale=pt_BR. Acesso em: 10 abr. 2025.

META. *Contas de adolescentes: novos recursos de privacidade, supervisão parental e bem-estar digital.* Meta Newsroom, 16 abr. 2025. Disponível em: https://about.fb.com/news/2025/04/introducing-new-built-in-restrictions-instagram-teen-accounts-expanding-facebook-messenger/. Acesso em: 15 jul. 2025.

META. *Propriedade intelectual nas plataformas da Meta.* 30 abr 2024b. Disponível em: https://www.meta.com/pt-br/help/policies/323433743488413/?srsltid=AfmBOopOteE7LzZZ5plewxdaxmnwEJjyl94cONMpGiOiQkahYDyM_lfR. Acesso em: 2 maio 2025.

MIGALHAS. STF tem sete votos para ampliar responsabilidade de redes sociais. *Migalhas*, [s. l.], 2025. Disponível em: https://www.migalhas.com.br/quentes/432512/stf-tem-sete-votos-para-ampliar-responsabilidade-de-redes-sociais. Acesso em: 16 jun. 2025.

MORAES, Ligia. Brasil ultrapassa média global no uso de inteligência artificial, mostra pesquisa. *Veja*, 14 jan. 2025. Disponível em: https://veja.abril.com.br/tecnologia/brasil-ultrapassa-media-global-no-uso-de-inteligencia-artificial-mostra-pesquisa/. Acesso em: 24 jun. 2025.

NEURORIGHTS FOUNDATION, 2023. Disponível em: https://neurorightsfoundation.org. Acesso em: 18 out. 2024.

NUNES, Dierle. Patrimônio e herança digital. In: *A reforma do Código Civil: artigos sobre a atualização da Lei nº 10.406/2002. /* org. Rodrigo Pacheco. – Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2025, p. 409-426.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Recommendation of the Council on Responsible Innovation in Neurotechnology. (2019)* Disponível em: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0457. Acesso em: 10 out. 2024.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). COMISSÃO JURÍDICA INTERAMERICANA. *Declaração da Comissão Jurídica Interamericana sobre Neurociência, Neurotecnologias e Direitos Humanos: Novos Desafios Jurídicos para as Américas* (CJI/DEC. 01 (XCIX-O/21))(2021b). Aprovada no 99º Período Ordinário de Sessões, 11 ago. 2021. Disponível em: https://www.oas.org/en/sla/iajc/docs/CJI-DEC_01-XCIX-O-21_POR.pdf. Acesso em: 15 jul. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL). Convenção das Nações Unidas sobre o Uso de Comunicações Eletrônicas em *Contratos Internacionais (Convenção de Comunicações Eletrônicas — ECC),* adotada em 23 nov. 2005. Nova York: ONU, 2005. Disponível em: https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications. Acesso em: 15 jul. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL). *Model Law on Electronic Signatures with Guide to Enactment 2001.* Viena: ONU, 2001. Disponível em: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures. Acesso em: 15 jul. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL). *Model Law on Electronic Commerce (with Guide to Enactment 1996)*. Viena: ONU, 1996. Disponível em: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce. Acesso em: 15 jul. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral (1989). *Convenção sobre os Direitos da Criança, adotada em 20 de novembro de 1989*. Nova Iorque: Organização das Nações Unidas, 1989. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em: 15 jul. 2025.

ORTEGA, Rodrigo. *Já dá para comprar 'vida eterna' de parentes via IA; você compraria?* TAB UOL, São Paulo, 31 ago. 2024. Disponível em: https://tab.uol.com.br/noticias/redacao/2024/08/31/conversar-com-parentes-mortos-via-ia-ja-e-realidade-para-quem-pode-pagar.htm?cmpid=copiaecola. Acesso em: 20 abr. 2025.

PONTES DE MIRANDA, Francisco Cavalcante. *Tratado de Direito Privado*. São Paulo: RT, 2013.

PORTO, Laura. A exclusão de informações: um novo olhar na era digital. *Migalhas*, 9 jul. 2024a. Disponível em: https://www.migalhas.com.br/coluna/reforma-do-codigo-civil/410844/a-exclusao-de-informacoes-um-novo-olhar-na-era-digital. Acesso em: 20 abr. 2025.

PORTO, Laura. A herança digital na proposta de atualização do Código Civil: protegendo seu patrimônio digital. *Migalhas*, 28 maio 2024b. Disponível em: https://www.migalhas.com.br/coluna/reforma-do-codigo-civil/408156/a-heranca-digital-na-proposta-de-atualizacao-do-codigo-civil. Acesso em: 5 abr. 2025.

PORTO, Laura. Neurodireitos: um olhar para o futuro presente na era digital. *Migalhas*, 25 mar. 2024c. Disponível em: https://www.migalhas.com.br/coluna/migalhas-notariais-e-registrais/404071/neurodireitos-um-olhar-para-o-futuro-presente-na-era-digital. Acesso em: 18 out. 2024.

PORTO, Laura. Quando a inteligência artificial imita a vida: a reforma do Código Civil. *Migalhas*, 14 abr. 2025a. Disponível em: https://www.migalhas.com.br/coluna/reforma-do-codigo-civil/428274/quando-a-inteligencia-artificial-imita-a-vida. Acesso em: 20 abr. 2025.

PORTO, Laura. Visão geral do novo Livro do Direito Civil Digital e seus principais fundamentos. In: PACHECO, Rodrigo (org.). *A reforma do Código Civil: artigos sobre a atualização da Lei nº 10.406/2002*. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2025b, p. 387-398.

PUBLIC CITIZEN. *Tracker: State Legislation on Intimate Deepfakes*. Washington, D.C.: Public Citizen, 2024. Disponível em: https://www.citizen.org/article/tracker-intimate-deepfakes-state-legislation/. Acesso em: 26 jun. 2025.

REINO UNIDO. Law Commission. *Smart contracts*. Londres, 2021. Disponível em: https://lawcom.gov.uk/project/smart-contracts/. Acesso em: 24 jun. 2025.

REINO UNIDO. *UK Jurisdiction Taskforce. Legal statement on cryptoassets and smart contracts*. Londres: UK LawTech Delivery Panel, novembro 2019. Disponível em: https://lawtechuk.io/reports/legal-statement-cryptoassets-smart-contracts. Acesso em: 15 jul. 2025.

REINO UNIDO. *AA v. Persons Unknown & Ors, [2019] EWHC 3556 (Comm),* High Court of Justice (Commercial Court), 13 Dec. 2019. Disponível em: https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html. Acesso em: 15 jul.

REINO UNIDO. *Online Safety Act 2023*, c. 50. Jornal Oficial do Reino Unido, 26 out. 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/contents. Acesso em: 24 jun. 2025.

REINO UNIDO. Information Commissioner's Office (ICO). *Age appropriate design: a code of practice for online services*. Londres: ICO, 2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 15 jul. 2025.

REINO UNIDO. *Data Protection Act 2018*. Londres: The National Archives, 2018. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Acesso em: 15 jul. 2025.

REINO UNIDO. *Age Appropriate Design Code*. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 22 nov. 2024.

RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Alex. *Neurotecnologia permitirá alterar funcionamento mental, diz cientista*. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-03/neurotecnologia-permitira-alterar-funcionamento-mental-diz-cientista#:~:text=Neurotecnologia%20permitirá%20alterar%20funcionamento%20mental%2C%20diz%20cientista,-Espanhol%20Rafael%20Yuste&text=O%20neurobiólogo%20espanhol%20Rafael%20Yuste,mais%20influentes%20neurocientistas%20da%20atualidade. Acesso em: 14 out. 2024.

SABINO, Marco Antônio C.; SOUZA, Gabriel Grigoletto Martins de. Alteração do Código Civil: regulamentação dos contratos digitais. *Jota*, 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/alteracao-do-codigo-civil-regulamentacao-dos-contratos-digitais. Acesso em: 20 out. 2024.

SALOMÃO, Luis Felipe; LEME, Elton (coord.); BACHUR, João Paulo (coord. técn.). *Moderação de conteúdo nas plataformas digitais*. Rio de Janeiro: Fundação Getulio Vargas, 2024. Disponível em: https://justica.fgv.br/sites/default/files/2024-12/estudo_moderacao_conteudo.pdf. Acesso em: 5 abr. 2025.

SALOMÃO, Luis Felipe. O projeto de atualização do Código Civil. In: *A reforma do Código Civil: artigos sobre a atualização da Lei nº 10.406/2002. /* org. Rodrigo Pacheco. – Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2025, p.15-20.

SANTOS, Gabriel Gonçalves. *Smart contracts: conceitos, limitações e potencialidades*. 2022. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte, 2022. Disponível em: https://repositorio.ufmg.br/bitstream/1843/57345/3/Smart%20Contracts%20Conceitos%2C%20limitações%20e%20potencialidades.%20Gabriel%20Gonçalves%20Santos.pdf. Acesso em: 5 abr. 2025.

SCHREIBER, Anderson. *Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. Direito & Internet*, v. 2, p. 277-305, 2015.

SEAGATE & IDC. *The Digitization of the World From Edge to Core*. Novembro, 2018. Disponível em: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 5 abr. 2025.

SINGAPURA. ORIONW LAW. Landmark Singapore Court of Appeal case on autonomous algorithmic trading: *Quoine Pte Ltd v B2C2 Ltd*, 2020. Disponível em: https://www.orionw.com/news-insights/landmark-singapore-court-of-appeal-case-on-autonomous-algorithmic-trading. Acesso em: 26 jun. 2025.

SOCIEDADE BRASILEIRA DE PEDIATRIA. *Menos telas, mais Saúde – Atualização 2024: manual de orientação para uso consciente de telas e dispositivos digitais por crianças e adolescentes*. Rio de Janeiro: SBP, 2024. Disponível em: https://www.sbp.com.br/fileadmin/user_upload/24604c-MO__MenosTelas__MaisSaude-Atualizacao.pdf. Acesso em: 24 jun. 2025.

SOUZA, Luiz Paulo Inteligência artificial já é capaz de clonar a personalidade de qualquer pessoa. *Veja*, 5 jan. 2025. Disponível em: https://veja.abril.com.br/tecnologia/inteligencia-artificial-ja-e-capaz-de-clonar-a-personalidade-de-qualquer-pessoa. Acesso em: 24 jun. 2025.

SZABO, Nick. *Smart contracts*. 1994. Disponível em: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Acesso em: 24 jun. 2025.

TALAMINI, Eduardo; CARDOSO, André Guskow. Smart contracts, "autotutela" e tutela jurisdicional. *Revista do Ministério Público do Estado do Rio de Janeiro*, nº 89, jul./set. 2023, p. 45-93. Disponível em: https://www.mprj.mp.br/documents/20184/4409950/Eduardo+Talamini_André+Guskow+Cardoso.pdf. Acesso em: 24 jun. 2025.

TEIXEIRA, Tarcísio. *Direito digital e processo eletrônico*. 8ª edição. Rio de Janeiro: Saraiva, 2024.

TIKTOK. *Diretrizes da Comunidade. TikTok Legal*, 2024. Disponível em: https://www.tiktok.com/community-guidelines/pt?lang=pt-BR. Acesso em: 01 jun. 2025.

UNIÃO EUROPEIA. *Processo C131/12 –Google Spain SL e Google Inc. vs Agencia Española de Protección de Datos e Mario Costeja González*. Julgado em 13 de maio de 2014. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=pt. Acesso em: 24 jun. 2025.

UNIÃO EUROPEIA. *Diretiva 2010/13/UE do Parlamento Europeu e do Conselho, de 10 de março de 2010*, sobre a coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros relativas à prestação de serviços de comunicação social audiovisual (Diretiva dos Serviços de Comunicação Social Audiovisual) *Jornal Oficial da União Europeia*, L 95, p. 1–24, 15 abr. 2010. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32010L0013. Acesso em: 24 jun. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 910/2014*, de 23 de julho de 2014, sobre identificação eletrónica e serviços de confiança para transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. *Jornal Oficial da União Europeia*, L 257, p. 73–114, 28 ago. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910. Acesso em: 26 jun. 2025.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (GDPR).* Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10 jan. 2025.

UNIÃO EUROPEIA. *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Official Journal of the European Union, L 130, p. 92–125, 17 May 2019. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790. Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA. *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).* Official Journal of the European Union, L 265, p. 1–66, 12 Oct. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925. Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho*, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). *Jornal Oficial da União Europeia*, L 277, p. 1–102, 27 out. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065. Acesso em: 24 jun. 2025.

UNIÃO EUROPEIA. *European Law Institute. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection.* Report of the European Law Institute, Project Number: P-2018-17. Approved by the ELI Council on 5 July 2022 and by the ELI Membership on 8 September 2022. Council Draft published on 8 September 2022 and Final Draft published on 16 February 2023. Disponível em: https://www.

europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf. Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act)*. Official Journal of the European Union, L, n. 2023/2854, p. 1–65, 22 Dec. 2023. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-CELEX%3A32023R2854. Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA *Diretiva (UE) 2024/1385 do Parlamento Europeu e do Conselho, de 14 de maio de 2024, sobre o combate à violência contra as mulheres e à violência doméstica*. *Jornal Oficial da União Europeia*, L 2024/1385, p. 1–36, 24 maio 2024a. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401385. Acesso em: 24 jun. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia*, L 1689, p. 1–102, 12 jul. 2024b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32024R1689. Acesso em: 24 jun. 2025.

UNIÃO EUROPEIA. COMMISSION OF THE EUROPEAN COMMUNITIES. *Communication from the Commission to the European Parliament and the Council on illegal and harmful content on the Internet*. COM(96) 483 final, Brussels, 16 Oct. 1996. Disponível em: https://www.europarl.europa.eu/doceo/document/A-4-1997-0098_EN.html Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA. *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). Official Journal of the European Union*, L 265, p. 1–66, 12 Oct. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925. Acesso em: 15 jul. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo aos mercados de criptoativos (MiCA), que altera os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937*. Jornal Oficial da União Europeia, L 150, 9 jun. 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32023R1114. Acesso em: 15 jul. 2025.

VAN DIJCK, J.; POELL, T.; DE WAAL, M. C. *The platform society: public values in a connected world.* New York: Oxford University Press, 2018.

VENTURA, Dora Fix. Um retrato da área de Neurociência e comportamento no Brasil. *Psicologia: Teoria e Pesquisa*, 2010, v. 26, p. 123. Disponível em: <https://doi.org/10.1590/S0102-37722010000500011>. Epub, 13 Dez 2010. Acesso em: 2 out. 2024.

VOLKSWAGEN DO BRASIL. *VW 70 anos | Gerações | VW Brasil*. [2 min]. 3 jul. 2023. Disponível em: https://www.youtube.com/watch?v=aMI54-kqphE. Acesso em: 10 abr. 2025.

WE ARE SOCIAL; MELTWATER. *Digital 2025: Global Overview Report*. Disponível em: https://datareportal.com/reports/digital-2025-global-overview-report. Acesso em: 4 abr. 2025.

X. *Políticas e regras do X.* 2024. Disponível em: https://help.twitter.com/pt/rules-and-policies. Acesso em: 15 jul. 2025.

X. *Como entrar em contato com o X para falar sobre a conta de um familiar falecido. 2025.* Disponível em: https://help.x.com/pt/rules-and-policies/contact-x-about-a--deceased-family-members-account. Acesso em: 20 abr. 2025.

YOUNG, Kimberly S.; ABREU, Cristiano N. *Dependência de internet em crianças e adolescentes: fatores de risco, avaliação e tratamento*. Porto Alegre: ArtMed, 2018.

YOUTUBE. *Políticas de Remoção de Conteúdo. Google Support* – YouTube, 2024. Disponível em: https://support.google.com/youtube/answer/2801941. Acesso em: 01 jun. 2025.

YUSTE, R., GOERING, S., ARCAS, B. et al. Four ethical priorities for neurotechnologies and AI. *Nature* 551, p. 159–163, 2017. Disponível em: https://www.nature.com/articles/551159a. Acesso em: 7 out. 2024.

FGV JUSTIÇA