SOUZAEAD
Revista Acadêmica Digital

ISSN 2595-5934



PERIODICIDADE
MENSAL

NOV 2026 EDIÇÃO Nº103

IDIOMAS
PORTUGUÊS E INGLÊS

QUALIS B3

CAPES

www.souzaeadrevistaacademica.com.br

SOUZAEAD
Revista Acadêmica Digital
ISSN 2595-5934
NOV 2026 EDIÇÃO Nº103

RESPONSABILIDADE CIVIL E INTELIGÊNCIA ARTIFICIAL: OS IMPACTOS DOS *DEEPFAKES* NOS DIREITOS DA PERSONALIDADE

CIVIL LIABILITY AND ARTIFICIAL INTELLIGENCE: THE IMPACTS OF DEEPFAKES ON PERSONALITY RIGHTS

VASCONCELLOS, Bernardo Diniz Accioli de[1]

RESUMO
O presente trabalho analisa os impactos jurídicos da tecnologia *deepfake* sob as óticas da responsabilidade civil, dos reflexos penais, da tutela eleitoral e da proteção infantojuvenil no ambiente digital. Com a popularização da inteligência artificial generativa, a manipulação de imagem e de voz atingiu níveis de hiper-realismo que desafiam os institutos tradicionais de proteção à pessoa humana. O estudo investiga as ofensas aos direitos da personalidade, como imagem, honra e identidade pessoal, tangenciando o surgimento do dano existencial. Sob o prisma da responsabilidade civil, discute-se a imputação subjetiva aos criadores e a aplicação analógica do artigo 21 do Marco Civil da Internet para a remoção extrajudicial de conteúdos íntimos sintéticos por parte dos provedores. No âmbito penal, abordam-se os crimes contra a honra, o estelionato por clonagem de voz e o artigo 218-C do Código Penal. Ademais, examina-se a incidência do chamado "ECA Digital" (Lei nº 15.211/2025) na repressão à pornografia sintética de menores e na atribuição de responsabilidade civil solidária aos pais e instituições de ensino. Por fim, avalia-se o impacto dessas mídias na higidez do processo eleitoral frente às resoluções de rotulagem do Tribunal Superior Eleitoral (TSE). Conclui-se que o ordenamento jurídico pátrio possui mecanismos dogmáticos suficientes para tutelar as vítimas, exigindo uma articulação coordenada e uma hermenêutica dinâmica entre as fontes cíveis, penais e constitucionais.
Palavras-chave: Responsabilidade Civil. *Deepfake*. Direitos da Personalidade. Direito Penal. ECA Digital. Direito Eleitoral.

ABSTRACT
This article analyzes the legal impacts of deepfake technology from the perspectives of civil liability, criminal consequences, electoral protection, and child and adolescent safety in the digital environment. With the popularization of generative artificial intelligence, the manipulation of image and voice has reached hyper-realistic levels that challenge traditional frameworks of human dignity protection. The study investigates violations of personality rights, such as image, honor, and personal identity, characterizing the emergence of existential damage. From a civil liability standpoint, it discusses the subjective imputation of creators and the analogical application of Article 21 of the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet) for the extrajudicial removal of synthetic intimate content by application providers. In the criminal sphere, it addresses crimes against honor, fraud via voice cloning, and Article 218-C of the Criminal Code. Furthermore, the paper examines the impact of the "Digital Child and Adolescent Statute" (ECA Digita) in suppressing synthetic

[1] Doutorando e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). baccioli@outlook.com.br

SOUZAEAD
Revista Acadêmica Digital
ISSN 2595-5934
NOV 2026 EDIÇÃO Nº103

pornography involving minors and assigning joint civil liability to parents and educational institutions. Finally, it evaluates the impact of these synthetic media on the integrity of the electoral process in light of the labeling resolutions issued by the Superior Electoral Court (TSE). It concludes that the domestic legal order possesses sufficient dogmatic mechanisms to protect victims, requiring a coordinated articulation and dynamic hermeneutics among civil, criminal, and constitutional sources.
Keywords: Civil Liability. Deepfake. Personality Rights. Criminal Law. Digital ECA. Electoral Law.

1. INTRODUÇÃO

A evolução exponencial da inteligência artificial generativa remodelou de forma irreversível os ecossistemas de informação e comunicação na contemporaneidade. Se, por um lado, a capacidade de sintetizar dados abriu horizontes sem precedentes para a criatividade e a eficiência industrial, por outro, deu origem a ferramentas sofisticadas de manipulação da verdade biológica e biométrica. Entre essas manifestações, os *deepfakes* destacam-se (GOODFELLOW et al., 2014; CITRON; CHESNEY, 2019) como mídias sintéticas de áudio e vídeo criadas por meio de Redes Adversárias Generativas (GANs) capazes de emular com precisão a aparência física e os padrões vocais de qualquer indivíduo. A problemática central reside na facilidade de acesso a tais tecnologias, permitindo que usuários comuns fabriquem contextos lesivos sem qualquer consentimento dos titulares dos direitos afetados.

Essa nova fronteira tecnológica tenciona os alicerces tradicionais (SARLET, 2012; DONEDA, 2021) do ordenamento jurídico, impondo uma revisão profunda nos critérios de tutela da dignidade humana no ambiente virtual. A criação de falsas narrativas audiovisuais não apenas desestabiliza a confiança nas interações sociais, mas atinge diretamente os direitos da personalidade (SCHREIBER, 2014; TEPEDINO, 2008), em especial a imagem, a honra e a identidade pessoal. Diante da pulverização instantânea de conteúdos sintéticos difamatórios ou fraudulentos nas redes sociais, os mecanismos clássicos de reparação cível e repressão penal enfrentam desafios operacionais complexos, agravados pelo anonimato e pela transnacionalidade das plataformas digitais.

O escopo do presente artigo consiste em analisar a arquitetura jurídica de

proteção à vítima e os critérios de imputação de responsabilidade aplicáveis à cadeia de criação e disseminação de mídias sintéticas não consensuais. Busca-se responder ao seguinte problema de pesquisa: de que maneira o ordenamento jurídico brasileiro pode tutelar as vítimas de *deepfakes* por meio da articulação sistemática entre a responsabilidade civil, os tipos penais vigentes e a proteção prioritária do Estatuto da Criança e do Adolescente?

Para solucionar essa indagação, adota-se uma abordagem analítico-dedutiva combinada com pesquisa bibliográfica e documental. O desenvolvimento estruturado do trabalho divide-se em quatro seções fundamentais: a análise do impacto dos *deepfakes* sobre a teoria dos direitos da personalidade; a dogmática da responsabilidade civil dos criadores e dos provedores sob a égide do Marco Civil da Internet; o enquadramento penal das fraudes e ofensas decorrentes da clonagem de voz e imagem; e a aplicação do ECA Digital (Lei nº 15.211/2025) para combater a pornografia sintética infantojuvenil no cenário escolar.

2. DESENVOLVIMENTO

2.1. A TECNOLOGIA *DEEPFAKE* E A DESCONSTRUÇÃO DA IDENTIDADE PESSOAL

A compreensão dos impactos jurídicos causados pelas mídias sintéticas pressupõe a delimitação de suas vertentes técnicas e operacionais. O fenômeno do *deepfake* subdivide-se em duas categorias principais de manipulação que operam de forma isolada ou combinada: a síntese de vídeo (substituição facial ou *face-swapping*) e a síntese de áudio (clonagem de voz ou *voice cloning*). Ambas se baseiam no processamento massivo de dados biométricos preexistentes da vítima, os quais alimentam redes neurais artificiais que aprendem a replicar expressões, trejeitos e inflexões tonais com fidelidade quase absoluta (GOODFELLOW et al., 2014).

A literatura técnica registra que a sofisticação dos modelos generativos reduziu drasticamente as barreiras de produção dessas mídias (CHESNEY; CITRON, 2019). Softwares antes restritos a laboratórios especializados passaram a integrar aplicações

de uso cotidiano, muitas delas gratuitas ou acessíveis mediante baixo custo. Esse fenômeno democratizou o acesso à criação audiovisual sintética e deslocou o problema jurídico do plano meramente tecnológico para o plano distributivo do risco social. Em outras palavras, a facilidade operacional amplia exponencialmente o universo de potenciais ofensores e multiplica a exposição das vítimas a danos reputacionais instantâneos e massivos. Sob tal perspectiva, a tutela jurídica não pode ignorar a assimetria estrutural entre a velocidade da propagação digital e o tempo ordinário das respostas institucionais.

Sob a ótica do Direito Civil, essa tecnologia provoca uma verdadeira ruptura na dimensão estática e dinâmica da identidade pessoal. A identidade não se resume ao registro civil (PERLINGIERI, 2002; SCHREIBER, 2014) ou aos caracteres biológicos imutáveis, mas engloba o patrimônio moral, o conjunto de atributos éticos, sociais e profissionais construídos pelo sujeito perante a coletividade. Ao permitir que a imagem ou a voz de um indivíduo sejam dissociadas de sua real vontade existencial para manifestar discursos falsos ou participar de atos degradantes, o *deepfake* aniquila autodeterminação informativa e a verdade pessoal, gerando um estado de desinformação biográfica crônica.

2.2. VIOLAÇÃO AOS DIREITOS DA PERSONALIDADE E A DOUTRINA DO DANO EXISTENCIAL

A construção dogmática dos direitos da personalidade (CUPIS, 2008; SCHREIBER, 2014) no Brasil encontra forte inspiração na tradição civil-constitucional europeia, que reconhece na pessoa humana não apenas um sujeito abstrato de relações patrimoniais, mas um centro axiológico merecedor de proteção integral (HIRONAKA, 2005). A jurisprudência brasileira consolidou progressivamente a ideia de que a imagem, a honra e a privacidade não constituem bens acessórios, mas projeções essenciais da personalidade. Em cenários de manipulação sintética, essa compreensão assume importância ainda maior, pois a lesão não decorre apenas da exposição indevida, mas da apropriação fraudulenta da identidade como instrumento de construção narrativa artificial. A vítima deixa de ser apenas objeto passivo da

divulgação para converter-se em personagem involuntária de uma ficção degradante.

Os direitos da personalidade, previstos nos artigos 11 a 21 do Código Civil de 2002, constituem garantias essenciais à proteção da dignidade do sujeito. A inserção da imagem ou da voz de uma pessoa em contextos sintéticos não autorizados configura uma violação direta e autônoma a esses bens jurídicos. O direito à imagem resguarda a expressão externa do corpo, enquanto o direito à voz protege a identidade sonora, sendo ambos irrenunciáveis e intransmissíveis (SCHREIBER, 2014). A jurisprudência pátria, consolidada na Súmula 403 do Superior Tribunal de Justiça, dispensa a prova de prejuízo na hipótese de publicação não autorizada da imagem com fins econômicos ou comerciais – orientação que a doutrina vem estendendo aos usos não consensuais em geral, com fundamento no caráter *in re ipsa* do dano moral.

No entanto, os danos decorrentes de mídias sintéticas hiper-realistas frequentemente transcendem o mero aborrecimento ou a simples ofensa à honra, transmudando-se em autêntico dano existencial. Este se caracteriza por uma alteração prejudicial e definitiva (SOARES, 2009; BODIN DE MORAES, 2003) na rotina de vida da vítima, comprometendo suas relações sociais, profissionais e afetivas. A doutrina civilista contemporânea aponta para a necessidade de conferir uma resposta a essas violações à dignidade da pessoa humana, conforme lição de Maria Celina Bodin de Moraes (2003, p. 112).

A literatura civilista contemporânea também tem reconhecido que a identidade pessoal constitui projeção existencial complexa da pessoa humana, não redutível a seus elementos registrais ou corporais. Nesse sentido, a manipulação sintética da personalidade por algoritmos de inteligência artificial produz lesões qualitativamente distintas das falsificações tradicionais, pois compromete simultaneamente a autenticidade biográfica, a autodeterminação e a credibilidade social do indivíduo. A circulação de conteúdos hiper-realistas produz ainda um efeito denominado "*liar's dividend*", pelo qual a própria existência dos *deepfakes* permite desacreditar provas audiovisuais verdadeiras, aprofundando a crise de confiança social (CITRON, CHESNEY, 2019).

A doutrina brasileira tradicionalmente compreende os direitos da personalidade

como cláusulas de tutela integral da pessoa humana, irradiadas da dignidade constitucional e dotadas de eficácia horizontal nas relações privadas (FACHIN, 2001). Em matéria de *deepfakes*, a violação assume caráter multifacetado, pois não apenas atinge a imagem isoladamente considerada, mas produz interferência abusiva na narrativa existencial construída pelo sujeito. O dano existencial decorrente da exposição sintética indevida pode traduzir perda de oportunidades profissionais, retraimento social e comprometimento duradouro da autonomia relacional.

A teoria contemporânea da responsabilidade civil também oferece ferramentas para refletir sobre deveres preventivos e precaucionais no ambiente digital. Em sociedades hiperconectadas, a reparação posterior nem sempre resta suficiente para recompor a integridade moral da vítima, razão pela qual ganha importância a tutela inibitória e a remoção célere do conteúdo ofensivo. A responsabilidade civil deixa de ser compreendida apenas como mecanismo reparatório e assume progressivamente função preventiva e dissuasória, especialmente em cenários de alta replicabilidade tecnológica (SCHREIBER, 2014; ROSENVALD, 2017).

Nas hipóteses de *deepfakes* com teor difamatório ou pornográfico, a mensuração da indenização deve ponderar o alcance da viralização, o grau de realismo da montagem e a vulnerabilidade da vítima, garantindo que o montante fixado atue como efetivo desincentivo à reiteração de condutas ilícitas no meio tecnológico.

2.3. A RESPONSABILIDADE CIVIL NA CADEIA DIGITAL: CRIADORES E PROVEDORES

Outro aspecto relevante refere-se à tensão entre liberdade de expressão e dever de proteção da personalidade. O ambiente digital frequentemente abriga discursos protegidos constitucionalmente, circunstância que impõe cautela para evitar mecanismos privados de censura indiscriminada. Todavia, a tutela constitucional da liberdade comunicativa não alberga manifestações fraudulentas conscientemente fabricadas para imputar fatos inexistentes ou explorar sexualmente a identidade alheia. O desafio hermenêutico consiste precisamente em distinguir conteúdos

opinativos, sátiras reconhecíveis e manifestações artísticas legítimas de montagens destinadas à fraude, à humilhação ou à manipulação social deliberada.

A atribuição da responsabilidade civil no cenário digital exige (MIRAGEM, 2023; DONEDA, 2021) a segregação de condutas entre o criador da mídia sintética e o provedor de aplicação que viabiliza a sua propagação. Em relação ao criador do *deepfake* lesivo, a responsabilidade civil é subjetiva (MIRAGEM, 2023), fundamentada no artigo 186 do Código Civil. Aquele que, dolosa ou culposamente, distorce a realidade para macular a reputação alheia pratica ato ilícito e responde integralmente pelas perdas e danos. Permanecem ali, intactos, os três pressupostos clássicos que De Page (1964) sistematizou para a responsabilidade aquiliana — conduta culposa, dano e nexo causal —, agora apenas reescritos sobre o suporte algorítmico: a culpa se manifesta na eleição de software cuja finalidade ostensiva é a falsificação biométrica, o dano se realiza na lesão a bem da personalidade e o nexo causal se prova pela rastreabilidade técnica do arquivo produzido. Contudo, a eficácia dessa responsabilização é rotineiramente mitigada pela dificuldade técnica de rastreamento do autor originário no ciberespaço.

Diante disso, ganha relevo o regime jurídico aplicável aos provedores de aplicação de internet (plataformas de redes sociais). O Marco Civil da Internet (Lei nº 12.965/2014) estruturou a responsabilidade por conteúdo de terceiros em seu artigo 19, exigindo, como regra geral, a prévia notificação judicial específica para a configuração da desobediência e consequente dever de indenizar da plataforma. Essa blindagem inicial visa resguardar a liberdade de expressão e impedir a censura prévia por parte de entes privados. O próprio artigo 19 foi objeto de revisão recente por parte do Supremo Tribunal Federal (Temas 987 e 533, STF), que restringiu as hipóteses de blindagem das Big Techs. A decisão da Corte, ao confrontar a constitucionalidade da norma, sinalizou uma transição relevante para um sistema que busca equilibrar a responsabilidade das plataformas com a garantia do acesso democrático à informação, consolidando as balizas que regerão a moderação de conteúdo no país nas próximas décadas.

Não obstante, a velocidade de disseminação dos *deepfakes* pornográficos

(*deepnudes*) exigiu uma válvula de escape protetiva. O artigo 21 do Marco Civil da Internet dispõe sobre uma importante exceção à necessidade de ordem judicial, prevendo a responsabilidade solidária do provedor que, após receber uma notificação extrajudicial formal da vítima ou de seu representante legal, deixa de promover de forma tempestiva a indisponibilização de conteúdos que contenham cenas de nudez ou de atos sexuais de caráter privado.

A doutrina civilista especializada defende a aplicação analógica e extensiva do artigo 21 para abarcar as mídias sintéticas pornográficas. Embora a cena íntima seja materialmente falsa, o impacto devastador sobre a privacidade e a projeção social do indivíduo é idêntico ao do vazamento de imagens reais (*revenge porn*). Exigir que a vítima de um *deepnude* aguarde a concessão de uma tutela de urgência em juízo para ver seu rosto desvinculado de um vídeo pornográfico significaria chancelar a perpetuação diária do dano à sua integridade psicofísica.

A problemática dos *deepfakes* demonstra que a tecnologia não opera em vazio normativo, mas interage permanentemente com categorias jurídicas historicamente consolidadas. A aparente novidade técnica não elimina a centralidade da dignidade da pessoa humana como eixo estruturante do sistema civil-constitucional brasileiro. Em vez de substituir a dogmática clássica, a inteligência artificial desafia sua capacidade adaptativa e sua vocação de tutela integral da pessoa.

2.4. CONTORNOS PENAIS: DO ESTELIONATO POR CLONAGEM DE VOZ AOS CRIMES CONTRA A HONRA

O debate comparado revela que diferentes ordens jurídicas têm buscado respostas específicas ao fenômeno. Alguns sistemas normativos priorizam mecanismos de transparência algorítmica e rotulagem obrigatória; outros apostam em regimes de responsabilização agravada para plataformas ou em tipos penais autônomos voltados às manipulações sintéticas maliciosas. Independentemente do modelo escolhido, observa-se consenso crescente quanto à inadequação de tratar o *deepfake* ofensivo como simples manifestação tecnológica neutra. Trata-se, antes, de instrumento potencialmente apto a produzir lesões massivas à confiança pública e aos

SOUZAEAD
Revista Acadêmica Digital
ISSN 2595-5934
NOV 2026 EDIÇÃO Nº103

direitos fundamentais.

Os ilícitos perpetrados por meio de inteligência artificial gerativa (CITRON; CHESNEY, 2019) não se limitam à esfera reparatória cível, ecoando com gravidade no Direito Penal. A versatilidade da tecnologia permite a subsunção (GRECO, 2022; NUCCI, 2024) de condutas sintéticas a diversos tipos penais clássicos e modernos do Código Penal Brasileiro.

No âmbito patrimonial, a técnica de clonagem de voz (*voice cloning*) tornou-se vetor principal para a execução de fraudes financeiras complexas. O agente delituoso, valendo-se de fragmentos de áudio extraídos de redes sociais públicas, sintetiza a voz de um familiar ou de um diretor de empresa e realiza chamadas telefônicas ou envia mensagens de áudio solicitando transferências bancárias ou depósitos via PIX em caráter de urgência. Essa conduta amolda-se perfeitamente ao crime de Estelionato, tipificado no artigo 171 do Código Penal:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa (BRASIL, 1940).

O *deepfake* atua aqui como o "artifício" ou "ardil" de alta fidelidade técnica, anulando a capacidade crítica da vítima média, que confia nos padrões acústicos ouvidos para efetivar o desfalque patrimonial.

Além disso, a falsificação audiovisual de discursos políticos ou declarações corporativas atrai a incidência imediata dos Crimes contra a Honra. A imputação falsa de um crime por meio de montagem hiper-realista configura Calúnia (art. 138, CP); a atribuição de fato ofensivo não criminoso que macula a reputação pública atrai o crime de Difamação (art. 139, CP); e a criação de montagens satíricas ou humilhantes que ataquem diretamente o decoro ou a dignidade da pessoa em seu foro íntimo caracteriza o delito de Injúria (art. 140, CP). Em todos esses casos, o ambiente virtual atua como causa de aumento de pena (art. 141, § 2º, CP), em razão da facilidade de propagação do conteúdo ilícito.

O emprego de inteligência artificial em práticas delitivas suscita ainda debates

sobre imputação subjetiva, autoria mediata e sofisticação dos meios executórios. Embora os tipos penais permaneçam formalmente aptos à subsunção das condutas, a investigação criminal enfrenta obstáculos inéditos relacionados à anonimização tecnológica, ao uso de servidores estrangeiros e à velocidade de circulação transnacional das evidências digitais. Esses desafios exigem coordenação institucional e atualização pericial contínua.

Por fim, no campo dos crimes sexuais, a Lei nº 13.718/2018 introduziu o artigo 218-C no Código Penal, punindo a conduta de divulgar, sem consentimento, material pornográfico. A aplicação do tipo penal aos *deepfakes* pornográficos é agasalhada pela jurisprudência, na medida em que o bem jurídico tutelado é a dignidade sexual e o direito à exclusividade da própria intimidade física, os quais são violados com igual intensidade diante da simulação computadorizada (NUCCI, 2024).

2.5. A HIPERVULNERABILIDADE INFANTOJUVENIL E O ECA DIGITAL

As consequências psicológicas experimentadas por crianças e adolescentes vítimas de pornografia sintética ou humilhação digital reiterada revelam especial gravidade. A literatura especializada em violência digital aponta que a exposição pública não consensual tende a produzir isolamento social, ansiedade e ruptura dos vínculos escolares, agravados pela permanência indefinida dos registros em ambiente virtual (CITRON, 2014). A tutela jurídica, portanto, deve articular medidas repressivas e restaurativas, privilegiando a rápida interrupção do dano e a reconstrução das condições de convivência saudável.

O desdobramento mais alarmante da popularização dos softwares generativos reside na vitimização de crianças e adolescentes. O ambiente escolar tornou-se um terreno fértil para práticas de *cyberbullying*, no qual alunos utilizam-se de aplicativos para inserir rostos de colegas de classe em imagens pornográficas de banco de dados, disseminando-as em grupos de mensagens instantâneas. Essa realidade impõe a aplicação imediata do princípio da prioridade absoluta e da proteção integral, diretrizes constitucionais corporificadas no Estatuto da Criança e do Adolescente (ECA - Lei nº 8.069/1990).

SOUZAEAD
Revista Acadêmica Digital
ISSN 2595-5934
NOV 2026 EDIÇÃO Nº103

No ECA, a criação de pornografia infantil sintética encontra severa punição criminal. Os artigos 240 e 241 do estatuto tipificam as condutas de produzir, publicar e disseminar material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. A alteração legislativa promovida pela Lei nº 11.829/2008 foi cirúrgica ao incluir no texto legal os termos "simulação" e "representação visual", sepultando discussões doutrinárias antigas: mesmo que o corpo retratado pertença a um adulto, ou seja, ainda gerado inteiramente por computador, a inserção do rosto de um menor configura o crime de pornografia infantojuvenil.

Na esfera cível e pedagógica, o ordenamento jurídico reage por meio da imputação da responsabilidade civil solidária aos pais ou responsáveis legais dos menores infratores que criam os *deepfakes*, nos estritos termos dos artigos 932, inciso I, e 933 do Código Civil. A escola, ao assumir o dever de custódia e vigilância sobre os alunos, responde pelos danos morais decorrentes do *bullying* e da propagação de ofensas digitais ocorridas ou articuladas sob suas dependências, devendo adotar posturas proativas de letramento digital e mediação de conflitos cibernéticos.

De todo modo, a proteção da criança e do adolescente no ambiente digital não pode limitar-se à repressão posterior do ilícito. A doutrina especializada tem insistido na necessidade de educação digital preventiva, formação ética e desenvolvimento de competências críticas para o uso responsável da tecnologia. O espaço escolar desempenha função decisiva nessa arquitetura protetiva, não apenas como *locus* de vigilância, mas como ambiente pedagógico voltado à cidadania digital e ao respeito aos direitos da personalidade.

3. CONSIDERAÇÕES FINAIS

A expansão da inteligência artificial generativa impõe ainda uma reflexão ética mais ampla acerca da autenticidade nas relações humanas. A erosão da confiança em registros audiovisuais compromete não apenas interesses individuais, mas a própria possibilidade de construção compartilhada da verdade social. O Direito Civil, historicamente vocacionado à tutela da pessoa e de seus vínculos existenciais,

desempenha papel central nesse cenário, oferecendo instrumentos aptos à recomposição do dano e à afirmação normativa da dignidade humana frente às novas tecnologias.

A incursão da inteligência artificial generativa na vida cotidiana por meio dos *deepfakes* descortinou um cenário de vulnerabilidade sem precedentes para os sujeitos de direito. A desmaterialização da prova biométrica e a capacidade de forjar a verdade audiovisual desafiam a estabilidade das relações jurídicas e exigem do Poder Judiciário uma postura hermenêutica dinâmica, apta a extrair a máxima eficácia das normas existentes.

Constatou-se que o Código Civil de 2002 oferece instrumentos dogmáticos aptos a amparar as vítimas, qualificando o *deepfake* não consensual como ato ilícito flagrante que atenta contra os direitos da personalidade e autoriza a fixação de indenizações por dano moral e existencial com caráter punitivo-pedagógico. Para assegurar a utilidade prática da tutela, a interpretação progressiva do artigo 21 do Marco Civil da Internet mostra-se indispensável, impondo aos provedores de aplicação o dever de remover mídias sintéticas íntimas mediante simples notificação extrajudicial.

Do mesmo modo, o aparato penal e a proteção especial do ECA Digital revelam-se suficientes para enquadrar as condutas criminosas — desde os estelionatos operados por clonagem de voz até os graves delitos de pornografia sintética infantojuvenil —, restando evidente que a ausência de uma legislação setorial específica sobre IA não significa anomia ou desamparo legal. Conclui-se, portanto, que a articulação coordenada entre a reparação cível, a punição criminal dos criadores e a responsabilização solidária de pais e estabelecimentos escolares constitui o caminho dogmático legítimo para mitigar os danos existenciais causados pelas mídias sintéticas e preservar a dignidade humana na era cibernética.

4. REFERÊNCIAS

BODIN DE MORAES, Maria Celina. *Danos à pessoa humana: uma leitura civil-*

constitucional do dano moral. Rio de Janeiro: Renovar, 2003.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. *Diário Oficial da União*, Brasília, DF, 31 dez. 1940.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto da Criança e do Adolescente Digital (ECA Digital). *Diário Oficial da União*, Brasília, DF, 18 set. 2025.

CHESNEY, Robert; CITRON, Danielle Keats. Deep Fakes: a looming challenge for privacy, democracy, and national security. California Law Review, v. 107, n. 6, 2019.

CITRON, Danielle Keats. Hate Crimes in Cyberspace. Cambridge: Harvard University Presso, 2014.

CUPIS, Adriano de. Os direitos da personalidade. Trad. Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DE PAGE, Henri. *Traité élémentaire de droit civil belge*: principes, doctrine, jurisprudence. 3e éd. Bruxelles: Bruylant, 1964, t. II.

FACHIN, Luiz Edson. Estatuto jurídico do patrimônio mínimo. Rio de Janeiro: Renovar, 2001.

GOODFELLOW, Ian et al. Generative Adversarial Nets. In: Advances in Neural Information Processing Systems, 2014.

GRECO, Rogério. Curso de Direito Penal. 24. ed. Rio de Janeiro: Impetus, 2022.

HIRONAKA, Giselda Maria Fernandes Novaes. Responsabilidade pressuposta. Belo

Horizonte: Del Rey, 2005.

MIRAGEM, Bruno. Responsabilidade civil. 4. ed. São Paulo: Revista dos Tribunais, 2023.

NUCCI, Guilherme de Souza. Código Penal comentado. 24. ed. Rio de Janeiro: Forense, 2024.

PERLINGIERI, Pietro. Perfis do Direito Civil. Rio de Janeiro: Renovar, 2002.

ROSENVALD, Nelson. As funções da responsabilidade civil: a reparação e a pena civil. 3 ed. São Paulo: Saraiva, 2017.

SCHREIBER, Anderson. *Direitos da Personalidade*. 3. ed. São Paulo: Atlas, 2014.

TEPEDINO, Gustavo. *Temas de Direito Civil*. 4. ed. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 11. ed. Porto Alegre: Livraria do Advogado, 2012.

SOARES, Flaviana Rampazzo. Dano existencial: uma leitura da responsabilidade civil por danos à existência. Porto Alegre: Livraria do Advogado, 2009.