PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO – PUC-SP
FACULDADE DE DIREITO

BRUNO JUSTO LAZZARINI

PROTEÇÃO DOS DIREITOS DE IMAGEM E NA PRODUÇÃO DE CONTEÚDOS POR INTELIGÊNCIA ARTIFICIAL GENERATIVA: DEEPFAKES, AVATARES DIGITAIS E OS LIMITES DO MARCO JURÍDICO BRASILEIRO

São Paulo
2025

Bruno Justo Lazzarini

PROTEÇÃO DOS DIREITOS DE IMAGEM E NA PRODUÇÃO DE CONTEÚDOS POR INTELIGÊNCIA ARTIFICIAL GENERATIVA: DEEPFAKES, AVATARES DIGITAIS E OS LIMITES DO MARCO JURÍDICO BRASILEIRO

Trabalho de conclusão de Curso, apresentado a Pontifícia Universidade Católica de São Paulo - SP, como parte das exigências para a obtenção do título de bacharel em direito.

São Paulo, 24 de novembro de 2025.

Prof. Dr. Adriano Ferriani

RESUMO

O presente trabalho analisa a proteção do direito de imagem diante da criação e disseminação de conteúdos sintéticos produzidos por inteligência artificial generativa, especialmente deepfakes e avatares digitais. As representações algorítmicas hiper-realistas, capazes de reproduzir traços físicos e vocais de pessoas reais sem qualquer captação direta, desafiam as categorias tradicionais do Direito Civil brasileiro e exigem releitura do artigo 20 do Código Civil, que disciplina o consentimento e o uso da imagem. A pesquisa, de natureza qualitativa e bibliográfica, fundamenta-se na análise de doutrina, jurisprudência, legislações nacionais (como o Marco Civil da Internet e a Lei Geral de Proteção de Dados) e debates regulatórios internacionais, buscando compreender como a autonomia sobre a própria identidade visual pode ser preservada em um ambiente digital marcado pela manipulação algorítmica. O estudo examina as principais questões jurídicas decorrentes da reprodução sintética de rostos e identidades, destacando que a mera manipulação não consentida – ainda que sem captação real – constitui violação ao direito da personalidade. Analisa-se também a cadeia de responsabilidade envolvendo usuários, plataformas digitais e desenvolvedores de inteligência artificial, evidenciando que, embora o ordenamento jurídico brasileiro disponha de mecanismos relevantes de tutela, persistem lacunas quanto à responsabilização de modelos treinados de forma opaca e à atuação preventiva dos intermediários tecnológicos. Casos recentes, nacionais e internacionais, ilustram a gravidade dos riscos associados aos deepfakes, como a disseminação de conteúdos sexuais não consensuais, fraudes vocais e usos políticos manipulativos. Por fim, o trabalho propõe reflexões sobre a necessidade de aperfeiçoamentos regulatórios voltados ao fortalecimento da proteção da identidade digital, à ampliação de deveres de transparência, segurança e mitigação de riscos pelos agentes tecnológicos e à harmonização entre inovação e direitos fundamentais. Defende-se que a efetiva tutela da imagem no contexto da inteligência artificial generativa depende da interpretação evolutiva do direito positivo e da incorporação de parâmetros técnicos e jurídicos aptos a enfrentar os desafios da era algorítmica.

Palavras-chave: Direito de imagem; Inteligência artificial generativa; Deepfakes; Responsabilidade civil; Proteção de dados pessoais.

ABSTRACT

This study examines the protection of image rights in the context of synthetic content generated by generative artificial intelligence, particularly deepfakes and digital avatars. Hyper-realistic algorithmic representations capable of reproducing physical and vocal features of real individuals without any direct capture challenge traditional categories of Brazilian Civil Law and require a reinterpretation of Article 20 of the Civil Code, which governs consent and the use of personal image. The research, qualitative and bibliographical in nature, is grounded in the analysis of doctrine, case law, national legislation (such as the Brazilian Internet Act and the General Data Protection Law), and international regulatory debates, seeking to understand how personal autonomy over one's visual identity can be preserved in a digital environment increasingly shaped by algorithmic manipulation. The study explores the main legal issues arising from the synthetic reproduction of faces and identities, emphasizing that non-consensual manipulation – even without real photographic capture – constitutes a violation of personality rights. It also analyzes the chain of liability involving users, digital platforms, and AI developers, demonstrating that although Brazilian law provides relevant protective mechanisms, significant gaps remain regarding the accountability of opaque artificial intelligence models and the preventive duties of technological intermediaries. Recent national and international cases illustrate the severity of the risks associated with deepfakes, such as the dissemination of non-consensual sexual content, voice-based fraud schemes, and manipulative political uses. Finally, the work proposes reflections on the need for regulatory improvements aimed at strengthening digital identity protection, expanding transparency and safety obligations for technological agents, and harmonizing innovation with fundamental rights. It argues that the effective safeguarding of image rights in the era of generative artificial intelligence depends on an evolutionary interpretation of existing law and on the incorporation of technical and legal parameters capable of addressing the challenges posed by algorithmic technologies.

Key-words: Image rights; Generative artificial intelligence; Deepfakes; Civil liability; Personal data protection.

SUMÁRIO

INTRODUÇÃO

Nas últimas décadas, a disseminação de ferramentas digitais capazes de criar, manipular e recombinar informações visuais transformou de modo profundo a forma como indivíduos se representam e são representados no ambiente virtual. A popularização recente das tecnologias de Inteligência Artificial generativa ("IAG") – especialmente aquelas voltadas à criação de imagens, vídeos e áudios sintéticos – intensificou esse movimento ao permitir que rostos, corpos, vozes e traços identitários de pessoas reais fossem reproduzidos com elevado grau de verossimilhança, muitas vezes sem qualquer participação ou consentimento do indivíduo retratado. Ferramentas como *MidJourney*, *DALL-E*, *Stable Diffusion* e outros modelos avançados de síntese de voz consolidaram um cenário no qual a identidade visual se tornou vulnerável à manipulação algorítmica, inaugurando desafios que extrapolam o campo tecnológico e alcançam diretamente a esfera dos direitos da personalidade.

A criação dos chamados deepfakes (vídeos hiper-realistas que simulam comportamentos, falas e gestos de pessoas reais) é um dos exemplos mais expressivos desse fenômeno. Ainda que inicialmente empregados em contextos recreativos ou experimentais, esses conteúdos tornaram-se gradualmente mais sofisticados e disseminados, produzindo impactos relevantes na esfera jurídica, política e social. Episódios envolvendo celebridades internacionais, como Scarlett Johansson[1] – cuja voz foi replicada sem autorização –, e Taylor Swift[2] – cuja imagem foi manipulada para fins de criação de conteúdos sexuais artificiais e disseminados viralmente –, ilustram os riscos inerentes ao uso indiscriminado dessas tecnologias e evidenciam a lacuna normativa existente quanto à proteção da imagem no ambiente digital contemporâneo.

O fenômeno também desafia as categorias jurídicas tradicionais do Direito Civil brasileiro. O direito de imagem, historicamente associado à captação e divulgação de fotografias ou filmagens reais, passa a ser tensionado pela criação de representações puramente artificiais, que não derivam de uma situação concreta, mas sim da análise estatística de grandes bases de dados. Essa mudança de paradigma provoca

[1] CNN BRASIL. Disputa entre Scarlett Johansson e OpenAI realça temor de Hollywood com IA. São Paulo, 21 maio 2024. Disponível em: https://www.cnnbrasil.com.br/entretenimento/disputa-entre-scarlett-johansson-e-openai-realca-temor-de-hollywood-com-ia/.

[2] FORBES BRASIL. O que o caso Taylor Swift nos alerta sobre os perigos da IA. São Paulo, 18 jan. 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/01/o-que-o-caso-taylor-swift-nos-alerta-sobre-os-perigos-da-ia/.

questionamentos relevantes: a reprodução sintética da imagem de alguém constitui violação quando não há captação direta? O consentimento previsto no art. 20 do CC aplica-se a avatares digitais e *deepfakes*? É possível exigir responsabilização de plataformas ou desenvolvedores quando o conteúdo ilícito é gerado por usuários anônimos ou por modelos treinados de maneira opaca?

A ausência de respostas legislativas claras acentua essas incertezas. Embora a Constituição Federal ("CF") assegure a proteção da imagem como direito fundamental, e o CC estabeleça mecanismos de tutela contra usos não autorizados, tais normas foram concebidas em um contexto no qual a imagem correspondia à reprodução fiel do corpo físico, e não a uma construção algorítmica. A Lei Geral de Proteção de Dados (Lei n° 13.709 – "LGPD"), por sua vez, introduziu salvaguardas importantes relacionadas ao tratamento de dados pessoais, incluindo informações biométricas, mas seu escopo ainda não contempla de modo direto a manipulação de identidades sintéticas criadas independentemente da coleta de dados sensíveis do titular.

Esse cenário revela um descompasso crescente entre a velocidade da evolução tecnológica e a capacidade de adaptação do ordenamento jurídico, produzindo insegurança tanto para titulares de direitos quanto para usuários, empresas e desenvolvedores envolvidos no ciclo de criação e disseminação desses conteúdos. Trata-se de um desafio que transcende a técnica e envolve a necessidade de resguardar a dignidade da pessoa humana em sua dimensão informacional e representacional, especialmente em uma sociedade marcada pela circulação massiva de imagens e pela construção constante de identidades digitais.

Nesse contexto, o presente trabalho tem como objetivo analisar criticamente a suficiência – ou insuficiência – dos mecanismos jurídicos brasileiros para tutelar o direito de imagem diante das novas possibilidades de criação sintética proporcionadas pela IAG.

Busca-se investigar de que modo as normas existentes se articulam com as tecnologias emergentes, quais lacunas se evidenciam na proteção da identidade visual, e quais caminhos interpretativos ou normativos podem contribuir para um equilíbrio mais adequado entre inovação tecnológica e proteção dos direitos fundamentais. Para isso, serão examinados os fundamentos do direito de imagem no ordenamento brasileiro, os impactos específicos das tecnologias de IA sobre esse direito e as alternativas regulatórias

debatidas no cenário internacional, especialmente na União Europeia, nos Estados Unidos e no Reino Unido.

A investigação adota abordagem crítica, interdisciplinar e comparada, com a finalidade de compreender de forma abrangente os desafios atuais e propor reflexões que permitam aperfeiçoar a tutela jurídica da imagem em um contexto de transformação tecnológica contínua. A centralidade da pessoa humana – ideia estruturante do Direito Civil – servirá de referência para avaliar a adequação das respostas normativas existentes e orientar possíveis caminhos futuros no tratamento das representações sintéticas produzidas por IA.

CAPÍTULO 1 – A Inteligência Artificial Generativa e a Reprodução Sintética da Imagem Humana

1.1. Conceito e funcionamento da IA generativa

A IAG representa uma categoria específica de sistemas algorítmicos capazes de produzir novos conteúdos a partir de padrões previamente aprendidos. Diferentemente das inteligências artificiais tradicionais, estruturadas para executar tarefas delimitadas por regras fixas ou por classificações previsíveis, as IAGs operam mediante modelos estatísticos complexos que conseguem recombinar informações, criar inferências e gerar resultados que simulam a criação humana. Essa distinção é essencial para compreender os desafios introduzidos por essas tecnologias, pois desloca o papel do algoritmo de mero executor para agente criador – ainda que sem vontade, consciência ou criatividade nos moldes humanos.

O funcionamento desses sistemas repousa principalmente em arquiteturas avançadas de redes neurais profundas, como os modelos de difusão e os grandes modelos de linguagem (*Large Language Models* – "*LLMs*"). As redes neurais reproduzem, em escala computacional, mecanismos inspirados no funcionamento biológico dos neurônios, permitindo que os algoritmos aprendam padrões complexos a partir de exposições extensivas a grandes quantidades de dados. Os modelos de difusão, por exemplo, geram imagens ao reconstruir padrões visuais a partir de um processo iterativo que parte do ruído até chegar a uma composição coerente. Já os *LLMs* analisam, interpretam e produzem linguagem natural com fluidez capaz de imitar a narrativa humana.

O treinamento desses sistemas depende da ingestão massiva de dados, coletados em grande parte por meio da raspagem automática de conteúdos disponíveis na internet. Fotografias, vídeos, textos, gravações de voz e até bases de dados biométricas são incorporados aos conjuntos de treinamento, muitas vezes sem transparência adequada sobre a origem, finalidade e critérios de seleção desses materiais. Essa etapa de coleta e processamento é crucial, pois define os limites do modelo e determina a qualidade das inferências produzidas.

Outro elemento fundamental para a operação da IAG é o mecanismo dos prompts, comandos inseridos pelo usuário que orientam o modelo na criação do resultado desejado.

Apesar disso, mesmo a interação humana por meio de prompts não garante previsibilidade plena, uma vez que a lógica interna do modelo – frequentemente descrita como uma "caixa-preta" – impede que se compreenda, em detalhes, como cada informação do *dataset*[3] influenciou o produto final. Esse grau de opacidade tecnológica dificulta tanto a auditoria quanto o controle jurídico dos outputs gerados.

Assim, embora a IAG seja frequentemente apresentada como uma criadora autônoma, seu funcionamento revela que seus resultados derivam da recombinação e reorganização de informações pré-existentes. Não há criação *ex nihilo*, mas sim um processo sofisticado de remixagem algorítmica – ponto essencial para a análise da produção de imagens sintéticas e das potenciais violações ao direito de imagem.

1.2. Deepfakes, avatares digitais e síntese de voz

O desenvolvimento de tecnologias generativas voltadas para vídeo, imagem e áudio deu origem aos chamados *deepfakes* – conteúdos hiper-realistas capazes de simular rostos, expressões, gestos e falas com precisão antes inimaginável. Originalmente concebidos como experimentos computacionais e, em alguns casos, utilizados em produções artísticas, essas técnicas rapidamente se popularizaram e passaram a integrar aplicações recreativas, publicitárias e também práticas ilícitas.

Deepfakes baseiam-se sobretudo em técnicas de *face swap* (troca de rostos) e *face reenactment* (recriação de rostos), pelas quais o rosto de uma pessoa é inserido no corpo de outra ou manipulado digitalmente para expressar gestos, falas e reações que jamais ocorreram. Paralelamente, a síntese de voz evoluiu a ponto de permitir clone digital de timbres, ritmos e entonações, o que expandiu ainda mais o espectro de manipulações possíveis. Avatares hiper-realistas, utilizados em ambientes virtuais, jogos e plataformas de comunicação e redes sociais, também se tornam cada vez mais verossímeis, reproduzindo características faciais e corporais de pessoas reais em três dimensões.

Casos como os mencionados de Scarlett Johansson e Taylor Swift evidenciam os riscos concretos da apropriação algorítmica da imagem e da reputação. Em contextos

[3] *Dataset*, em inglês, é o nome dado a um conjunto de dados organizados para alimentar, modelar e treinar IAGs.

políticos, deepfakes já foram utilizados para simular discursos e ações de figuras públicas de alta relevância, levantando preocupações sobre desinformação e uso estratégico dessas manipulações.

A distinção entre usos recreativos, artísticos e ofensivos é relevante, mas insuficiente para eliminar os riscos. O fenômeno dos *non-consensual deepfakes* (*deepfakes* não-consensuais), sobretudo aqueles de caráter sexual, configura uma das formas mais graves de violência digital contemporânea, com impactos psicológicos, sociais e reputacionais profundos. A facilidade de criação e difusão, aliada à dificuldade de remoção e rastreamento, intensifica a vulnerabilidade das vítimas.

Ao permitir que identidades sejam simuladas com extraordinária precisão, essas tecnologias ampliam sobremaneira os desafios jurídicos relacionados ao direito de imagem, razão pela qual sua análise demanda atenção específica nos capítulos seguintes.

1.3. A transformação da identidade visual no ambiente digital

O avanço das tecnologias generativas transformou o conceito de identidade visual, que deixou de estar exclusivamente vinculado à representação direta do corpo físico e passou a incorporar dimensões puramente sintéticas. A imagem de uma pessoa, antes limitada ao seu retrato captado por câmera ou vídeo, pode agora existir como uma construção algorítmica independente da materialidade do indivíduo.

Nesse contexto surge a noção de "imagem-síntese", expressão que designa representações visuais produzidas artificialmente, mas que preservam elementos essenciais da aparência de uma pessoa real. A imagem-síntese não é uma fotografia; é uma projeção algorítmica que se aproxima do verossímil sem depender de qualquer ato humano de captação – desafiando a definição tradicional de imagem, concebida pela doutrina civilista a partir da ideia de reprodução fiel da figura física.

A identidade digital, composta por traços, atributos e representações que circulam no ambiente virtual, ganha centralidade nesse processo. Reputação, credibilidade e presença online tornam-se extensões inseparáveis da personalidade, sendo profundamente afetadas pela difusão de conteúdos sintéticos. A autodeterminação informacional, isso é, o poder de controlar como a própria imagem é utilizada e

apresentada, torna-se elemento-chave para compreender os impactos dessa nova realidade.

A diluição da fronteira entre o real e o artificial intensifica efeitos sociais importantes. No ambiente hiperconectado, manipulações se espalham com rapidez, alcançando milhões de pessoas em minutos. A viralização confere aparência de verdade ao que é falso, reforçando preconceitos, distorções e narrativas enganosas.

Essa transformação do conceito de identidade exige que o Direito repense seus instrumentos de proteção, reconhecendo que a imagem, hoje, não se limita a fotografias tradicionais, mas inclui também representações algorítmicas capazes de produzir efeitos reais sobre a esfera pessoal, social e patrimonial do indivíduo.

1.4. Riscos jurídicos e sociais da manipulação algorítmica da imagem

A manipulação algorítmica da imagem acarreta riscos significativos que ultrapassam a mera esfera tecnológica e incidem diretamente sobre a dignidade, a honra e a intimidade da pessoa humana. A capacidade de gerar representações convincentes facilita a criação de conteúdos enganosos, fraudulentos ou difamatórios, que podem produzir danos psicológicos, morais e patrimoniais de grande magnitude.

Entre os riscos mais graves está a disseminação de *deepfakes* de caráter sexual não consensual, utilizados como forma de violência digital e instrumento de humilhação, controle ou vingança. A fabricação de discursos falsos em ambiente político também representa ameaça concreta à integridade do debate público e à confiança nas instituições democráticas.

Além disso, golpes e fraudes que utilizam clones de voz ou vídeos manipulados vêm se tornando mais frequentes, como em casos de extorsão e estelionato em que criminosos simulam a fala de familiares para solicitar transferências financeiras. Essas práticas, conhecidas como voice scams, ilustram a dimensão prática e imediata dos perigos envolvidos.

Do ponto de vista estrutural, a IAG pode reproduzir ou amplificar vieses discriminatórios presentes nos dados que alimentam os modelos, afetando de forma desproporcional grupos vulneráveis. A ausência de transparência e mecanismos de

controle eficiente dificulta a responsabilização dos agentes envolvidos, ao mesmo tempo em que compromete a eficácia das medidas de remoção e contenção.

Em síntese, os riscos jurídicos e sociais decorrentes das manipulações algorítmicas impõem a necessidade de respostas normativas capazes de proteger a imagem e a dignidade da pessoa humana, preparando o terreno para a análise dogmática e jurídica que será desenvolvida no próximo capítulo.

CAPÍTULO 2 – O Direito de Imagem no Ordenamento Jurídico Brasileiro

2.1. O direito de imagem como direito da personalidade

O direito de imagem ocupa posição central no conjunto dos direitos da personalidade e se relaciona diretamente com a proteção da dignidade humana. Tradicionalmente compreendido como a prerrogativa de controlar a forma pela qual a própria figura é representada, difundida e apropriada por terceiros, esse direito ultrapassa a mera preocupação estética ou privada e se conecta à autonomia do indivíduo na construção de sua identidade social. A imagem, enquanto manifestação externa da pessoa, participa de sua projeção no mundo e influencia a percepção coletiva sobre seus atributos, reputação e comportamento, razão pela qual sua tutela assume caráter estrutural dentro do Direito Civil contemporâneo

A doutrina civilista destaca que a imagem envolve tanto dimensões físicas – como retratos e gravações – quanto elementos simbólicos que integram a individualidade. Pablo Stolze Gagliano e Rodolfo Pamplona Filho conceituam o direito de imagem como "*a expressão exterior sensível da individualidade humana*", ou seja, a projeção visível da personalidade, digna de tutela jurídica.[4] Como complementa Carlos Alberto Bittar o direito de imagem "[c]onsiste *no direito que a pessoa tem sobre a sua forma plástica e respectivos componentes distintos (rosto, olhos, perfil, busto) que a individualizam no seio da coletividade. Incide, pois, sobre a conformação física da pessoa, compreendendo esse direito um conjunto de caracteres que a identifica no meio social. Por outras palavras, é o vínculo que une uma pessoa à sua expressão externa* [...]".[5]

[4] GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo Curso de Direito Civil: parte geral. São Paulo: Saraiva, 2002, p.183
[5] BITTAR, Carlos Alberto. Os direitos da personalidade. Rio de Janeiro, Forense, 2ª ed., 1995, p.87

Silvio Rodrigues, de forma clássica, pontua que "*a imagem de uma pessoa constitui, obviamente, um direito da personalidade*" inerente a todo indivíduo, por ser expressão exterior sensível da individualidade[6]. Trata-se de direito absoluto, extrapatrimonial, inalienável e irrenunciável, conforme estabelecido no art. 11 do CC.

> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Essa leitura revela-se especialmente relevante diante das tecnologias de IAG, que tornam possível a criação de representações sintéticas dotadas de alto grau de verossimilhança. A tensão entre a concepção clássica do direito de imagem e as novas possibilidades de manipulação e reprodução algorítmica exige uma reinterpretação cuidadosa dos limites e do alcance dessa tutela.

2.2. Previsão constitucional e tratamento no Código Civil

O arcabouço jurídico brasileiro protege a imagem em diferentes níveis normativos. No plano constitucional, o art. 5º, inciso X, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem, atribuindo ao titular o direito de buscar reparação pelos danos decorrentes de violações. Essa previsão reflete a compreensão de que a imagem integra o núcleo essencial da personalidade, cuja preservação é indispensável ao pleno exercício da dignidade humana.

No plano infraconstitucional, os arts. 20[7] e 21[8] do CC estabelecem que a utilização ou divulgação da imagem depende de autorização do retratado, ressalvadas hipóteses de interesse público ou figuração necessária. O regime jurídico construído a partir dessas normas pressupõe, contudo, uma noção clássica de imagem fundada na captação direta do corpo físico. Fotografias, filmagens e representações reais eram, até recentemente, o foco principal da proteção.

---

[6] RODRIGUES, Silvio. Direito Civil: parte geral. 34.ed., São Paulo: Saraiva, 2003, p.74

[7] Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

[8] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Ocorre, entretanto, que a emergência das representações sintéticas – como deepfakes e avatares digitais – revela a insuficiência desse modelo, pois a construção artificial da imagem dispensa qualquer ato de captação real. Ainda que o ordenamento não contenha previsão específica para essas situações, a jurisprudência brasileira tem reconhecido que o uso indevido da imagem, mesmo sem finalidade comercial, configura ilícito civil sempre que causar constrangimento, exposição indevida ou violação à autodeterminação do titular. O Superior Tribunal de Justiça ("STJ"), por meio da Súmula 403, consolidou o entendimento de que "*independe de prova do prejuízo a indenização pela publicação não autorizada da imagem de pessoa com fins econômicos*".

Esse entendimento fornece base para uma interpretação extensiva do regime civil em direção às novas tecnologias, devendo o consentimento ser interpretado com cautela e preferência pelo consentimento expresso e informado, sobretudo no ambiente digital.[9]

2.3. Modalidades de imagem: retrato, atributo e imagem-síntese

A doutrina brasileira clássica desdobra o conteúdo do direito de imagem em diferentes modalidades. Duas formas básicas são consensualmente reconhecidas: a imagem-retrato e a imagem-atributo.[10] A imagem-retrato corresponde à representação física e visível da pessoa – sua figura, fisionomia ou aparência externa identificável, que., como explica Luiz Alberto David Araújo, trata-se do direito relativo à reprodução gráfica da figura humana (por fotografia, desenho, filmagem etc.), abrangendo tudo que singulariza a aparência física da pessoa.[11] Já a imagem-atributo refere-se à projeção moral ou o "*retrato social*" da pessoa, ou seja, ao conjunto de atributos, características e qualidades pelas quais o indivíduo é reconhecido socialmente.

---

[9] CANHADAS FILHO, Gilberto; BRITO, Ana Carolina Ferreira de Melo. A inteligência artificial e os limites no uso do direito de imagem. Migalhas, 18 jul. 2023. Disponível em: https://www.migalhas.com.br/depeso/390067/a-inteligencia-artificial-e-os-limites-no-uso-do-direito-de-imagem

[10] SILVÉRIO, Michele de Cassia Tesseroli. O contrato de licença de uso de imagem e o direito do trabalho. 2004. Monografia (Bacharelado em Direito) — Universidade Federal do Paraná, Setor de Ciências Jurídicas, Curitiba, 2004. Disponível em: https://acervodigital.ufpr.br/xmlui/bitstream/handle/1884/48206/M456.pdf?sequence=1&isAllowed=y#:~:text=%E2%80%9CO%20direito%20%C3%A0%20imagem%20possui,A%20imagem%2C%20assim%2C%20tem%20duas

[11] ARAÚJO, Luiz Alberto David de. Curso de Direito Constitucional. Saraiva. São Paulo:l998, p.84, in ZANAIGHI, Domingos Sávio. Nova Legislação Desportiva - Aspectos Trabalhistas. LTr. São Paulo: 2001; e ARAUJO, Luiz Alberto David. A proteção constitucional da própria imagem. Dissertação de Mestrado. 1989. p. 31

Além dessas duas espécies, alguns autores reconhecem uma terceira modalidade, denominada imagem-biográfica. A referência aqui é à representação global da pessoa em sua trajetória de vida, abrangendo, por exemplo, as narrativas biográficas, filmes ou obras que retratam a história de alguém. A ilustre professora Maria Helena Diniz inclui expressamente essa hipótese ao conceituar a imagem. Para ela, a tutela da imagem abrange: a) "*a representação física da pessoa, como um todo ou em partes*" (imagem-retrato); b) "*o conjunto de atributos cultivados pela pessoa, reconhecidos socialmente*", refletindo a visão social do indivíduo (imagem-atributo); e c) *a* "*reprodução biográfica, que não pode conter dados mentirosos, sob pena de responsabilidade civil por dano moral e, até mesmo, patrimonial*".[12]

Diniz exemplifica esta terceira categoria mencionando a "*reprodução, romanceada em livro, filme, ou novela, da vida de pessoa de notoriedade*".[13] Nesses casos, proteção jurídica da imagem impede publicações biográficas não autorizadas que deturpem a verdade pessoal do biografado.

Em suma, a imagem-síntese corresponderia à síntese da identidade da pessoa em sua dimensão histórica e valorativa, garantindo-se ao indivíduo o direito de não ter sua história divulgada de modo falso ou sem consentimento. Vale notar que alguns juristas questionam se essa terceira modalidade não se confunde com outros direitos (como honra ou identidade), mas a classificação em três categorias serve para enfatizar que a proteção da imagem pessoal vai além do aspecto físico, abrangendo também a dimensão subjetiva e contextual da figura do indivíduo.

2.4. Consentimento e limites ao uso da imagem

É sabido que o consentimento constitui elemento estruturante da proteção do direito de imagem, funcionando como instrumento de autodeterminação do titular sobre o uso e a divulgação de sua figura. O CC, por meio do caput do art. 20, dispõe que salvo autorização da pessoa, ou necessidade de justiça ou ordem pública, a divulgação ou utilização da imagem pode ser proibida judicialmente, sem prejuízo de indenização, caso

[12] DINIZ, Maria Helena, Direito à imagem e sua tutela, In: BITTAR Eduardo C. B.; ALMEIDA, Silmara J. A. Chinelato e (coords). Estudos de direito de autor, direito da personalidade, direito do consumidor e danos morais. Forense Universitária, 2002. p. 79 e 80

[13] DINIZ, Maria Helena. Curso de direito civil brasileiro, volume 1: teoria geral do direito civil. 32. ed. São Paulo: Saraiva, 2015, p. 147.

atinja a honra, boa fama ou respeitabilidade do retratado, ou se for utilizada com fins comerciais. Isso significa que publicar foto ou retrato de alguém sem permissão constitui ilícito civil, especialmente se houver intuito comercial ou dano à reputação.

No entanto, a lógica do consentimento foi concebida em ambiente analógico e enfrenta dificuldades relevantes diante das imagens sintéticas. Como autorizar a manipulação de uma imagem que nunca existiu como fotografia ou vídeo real? A autorização concedida para uso de fotografias tradicionais abarca também representações artificiais? É possível consentir validamente com a criação de avatares hiper-realistas que extrapolam a aparência real do indivíduo? Essas questões demonstram que a estrutura clássica do consentimento não se ajusta integralmente às práticas possibilitadas pela IAG.

O STJ já assentou, por meio da Súmula 403, que, via de regra, exige-se consentimento expresso para uso da imagem; apenas excepcionalmente admite-se um consentimento tácito ou presumido, o qual deve ser interpretado de forma restrita e cautelosa. Nesse sentido, um exemplo de consentimento tácito ocorre em situações em que a própria pessoa se coloca voluntariamente em contexto público ou de notoriedade (como participar de um evento sendo fotografada publicamente). Ainda assim, tal consentimento implícito não é irrestrito e não autoriza usos distorcidos ou comerciais sem aval. Por outro lado, o consentimento expresso é a autorização clara, normalmente escrita ou registrada, permitindo determinado uso específico da imagem (como em contratos de licenciamento para publicidade).

Além disso, discute-se o consentimento informado no meio digital. Isso é, com a disseminação de fotos em redes sociais e plataformas online, é essencial que o titular seja adequadamente informado sobre a finalidade e alcance do uso de sua imagem antes de consentir. Autores contemporâneos traçam um paralelo entre as exigências de transparência informativa do art. 9º da LGPD e os deveres de esclarecimento no licenciamento civil da imagem: deve-se explicitar a finalidade, o contexto, a duração do uso e demais detalhes, garantindo que a pessoa consinta de forma livre e consciente.[14] Em qualquer caso, a ausência de consentimento válido torna o uso da imagem indevido: simples assim.

[14] BRESCIANI, Felipe Passos. Proteção do direito à imagem como dado pessoal e como direito da personalidade: um estudo comparativo. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) — Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2023. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/41017

Portanto, os limites ao uso da imagem são pautados pelo respeito à vontade do titular, admitindo-se exceções estritas (como finalidades jornalísticas, judiciais ou de segurança pública), e havendo responsabilização civil toda vez que a imagem for explorada sem anuência ou extrapolando os fins consentidos.

2.5. A interface com a LGPD e a proteção de dados biométricos

No cenário atual, o direito civil à imagem conecta-se intimamente com a LGPD. Isso porque a imagem de uma pessoa, quando armazenada ou divulgada em meios digitais, constitui dado pessoal – e, especificamente, dado biométrico quando se refere a características físicas que permitem identificá-la (por exemplo, fotografias do rosto utilizadas para reconhecimento facial).

A LGPD classifica dados biométricos como dados pessoais sensíveis (art. 5º, I e II)[15], o que acarreta um nível mais elevado de proteção. Na prática, isso significa que o tratamento de imagens capazes de identificar alguém deve observar os princípios e requisitos da lei de dados, sob pena de ilicitude.

Dentre os princípios da LGPD aplicáveis, destacam-se (i) a finalidade (uso da imagem apenas para propósitos legítimos, explícitos e informados ao titular); (ii) a necessidade (limitação do uso ao mínimo indispensável); (iii) a transparência (informar claramente o titular acerca do tratamento de sua imagem/dados); e (iv) a segurança (adoção de medidas para proteger esses dados contra acessos não autorizados).

Além disso, o tratamento de dado pessoal sensível somente é lícito nas hipóteses taxativas do art. 11 da LGPD, que incluem principalmente o consentimento específico e destacado do titular ou uma base legal excepcional (como cumprimento de obrigação legal, tutela da saúde, garantia de prevenção à fraude, exercício regular de direito, entre outras).

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

[15] Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]

> 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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> 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.

No contexto da imagem, via de regra será exigido o consentimento expresso do titular para uso de sua figura quando esta constituir dado pessoal – o que se alinha à necessidade de autorização prevista no CC. Ressalte-se que, mesmo quando a utilização da imagem possa se basear em alguma exceção da LGPD (por exemplo, uso jornalístico ou artístico, que são dispensados de consentimento pela própria LGPD em certos casos – art. 4º, II, c)[16], ainda assim devem ser respeitados os direitos de personalidade correlatos.

A proteção de dados biométricos reforça a tutela civil da imagem, pois impede, por exemplo, o armazenamento indiscriminado de fotos de rostos em bancos de dados ou sistemas de reconhecimento facial sem respaldo legal e sem informar os afetados. Conforme aponta a doutrina, há clara correspondência entre os deveres de transparência no uso civil contratual da imagem e aqueles exigidos para tratamento de dados pessoais:

[16] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: II - realizado para fins exclusivamente: a) jornalístico e artísticos; [...]

em ambos, busca-se garantir que o titular mantenha controle sobre o uso e a exploração de sua imagem, seja ela encarada como dado pessoal ou atributo da personalidade.

Em suma, a interface entre a LGPD e o direito civil evidencia que a exploração da imagem no meio digital deve observar simultaneamente as duas ordens normativas, a fim de assegurar uma tutela mais completa: a imagem como dado pessoal sensível somente pode ser utilizada dentro dos limites permitidos pela lei de dados, sob pena de sanções administrativas, e também fora desses limites o lesado pode buscar a via judicial civil por dano à personalidade.

CAPÍTULO 3 – IA Generativa e os Desafios para a Tutela Jurídica da Imagem

3.1. Interpretação Crítica do Art. 20 do Código Civil diante de Deepfakes e Imagens Geradas por IA

O art. 20 do CC[17] consagra a proteção ao direito de imagem, dispondo que, salvo consentimento ou necessidade para a justiça ou ordem pública, a divulgação de escritos, transmissão de palavra ou publicação/exposição da imagem de uma pessoa pode ser proibida a pedido do interessado, sem prejuízo de indenização se lhe atingirem a honra, reputação ou se destinarem a fins comerciais, como explica Filipe Medon.[18] Essa redação tem raízes históricas na tutela da imagem relacionada à honra e ao uso comercial, refletindo preocupações da época da fotografia analógica. Contudo, diante de deepfakes e imagens sintéticas geradas por IA, doutrinadores apontam a necessidade de uma interpretação crítica e atualizada desse dispositivo.

Antes de tudo, é preciso reconhecer que o direito à imagem é autônomo, não se confundindo com o direito à honra ou à privacidade. Parte da doutrina clássica entendia que apenas haveria ilícito na veiculação da imagem alheia quando houvesse ofensa à honra – a chamada teoria da honra, segundo a qual "*o retrato que nada tiver de insultante,*

[17] Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

[18] MEDON, Filipe. O direito à imagem na era das deepfakes. Revista Brasileira de Direito Civil – RBDCivil, v.27, p. 251-277, jan./mar. 2021. Disponível em: rbdcivil.ibdcivil.org.br. Acesso em: 15 out. 2025.

nada tem de repreensível".[19] O CC ainda padece desse viés ao mencionar ofensa à reputação e uso comercial como gatilhos para reparação, o que é visto como um equívoco conceitual. Modernamente, com base na CF (art. 5º, X), prevalece o entendimento de que a simples utilização não autorizada da imagem de alguém, por si só, configura violação do direito de imagem, independentemente de haver insulto ou lucro envolvido. Trata-se de direito da personalidade ligado à dignidade da pessoa, conferindo a cada indivíduo controle sobre qualquer representação de sua figura identificável (MEDON, 2021).

Nesse contexto, os deepfakes – montagens ultrarrealistas que recriam a face, voz ou ações de uma pessoa via algoritmos – representam um desafio paradigmático. Filipe Medon (2021) ainda observa que as deepfakes se inserem em um contexto de "reconstrução digital" da imagem, sintomáticas de uma mudança de paradigma na tutela do direito à imagem. Diferentemente de meras fotografias ou montagens rudimentares, as deepfakes podem convencer o público de que alguém disse ou fez algo que jamais ocorreu, exacerbando o potencial lesivo da divulgação não autorizada da imagem. Diante disso, a interpretação do art. 20 do CC requer ênfase no consentimento como elemento central: a inovação tecnológica reforça a importância de só se admitirem utilizações da imagem alheia quando autorizadas pelo titular (ou por outra exceção legal).

Assim, mesmo que uma *deepfake* não seja abertamente difamatória, a mera manipulação não consentida da aparência de alguém já fere seu direito personalíssimo, por violar sua autonomia sobre a própria representação. "*A violação da imagem atinge valores basilares da personalidade e da dignidade humana, ainda que não haja dano material ou abalo à honra comprovado*" (MEDON, 2021). Em outras palavras, a tutela jurídica deve abranger não apenas a proteção contra difamação via imagem, mas qualquer uso indevido da imagem real ou simulada de uma pessoa. Logo, frente às deepfakes, o art. 20 CC deve ser lido à luz do princípio constitucional da dignidade e dos direitos da personalidade, garantindo ao lesado medidas inibitórias e reparatórias independentemente de prova de dano concreto, conforme veremos adiante.

Outro ponto de releitura crítica diz respeito às exceções do art. 20 – "administração da justiça" e "manutenção da ordem pública". Tais hipóteses excepcionais foram concebidas para permitir, por exemplo, divulgação de imagens de procurados pela

[19] LOUREIRO, Henrique Vergueiro. Direito à imagem. Dissertação (Mestrado) – Pontifícia Universidade Católica de São Paulo – PUC/SP, São Paulo, 2005. p. 103.

polícia ou uso da imagem em julgamentos. Com deepfakes, porém, questiona-se se poderiam surgir situações justificadas de utilidade pública. Em princípio, criações de IA com rostos reais não se enquadram nas exceções e não deveriam ser divulgadas sem consentimento, a menos que atendam a um intresse público preponderante e legítimo (como sátiras políticas protegidas pela liberdade de expressão, discutidas na Seção 3.5). No geral, a doutrina reforça que o recurso a *deepfake* deve respeitar limites estritos e, na dúvida, prevalece o direito à não-exposição da imagem.

Por fim, vale destacar a tutela post mortem da imagem frente às deepfakes. O parágrafo único do art. 20 do CC determina que, em caso de pessoa falecida ou ausente, cabe ao cônjuge, ascendentes ou descendentes zelar pelo uso da imagem. A IA já permite a chamada "ressurreição digital" de personalidades falecidas – a exemplo do caso em que a cantora Elis Regina, falecida em 1982, foi recriada digitalmente para um comercial em 2023. Nesse caso, embora a campanha publicitária tenha contado com anuência dos familiares, a situação ilustra a necessidade de consultar os herdeiros para qualquer uso póstumo da imagem (MEDON, 2021). Não havendo disposição em vida da pessoa, cumpre aos sucessores autorizar ou negar tais reproduções algorítmicas, sob pena de violação legal. A doutrina aponta que cabe ao legislador e aos tribunais fixar os limites dessa prática, garantindo que a memória e vontade presumida do falecido sejam respeitadas.

Em suma, a interpretação crítica do art. 20 frente às deepfakes exige reforçar o consentimento e a dignidade humana como eixos centrais, superando visões ultrapassadas e assegurando proteção efetiva contra essas novas formas de violação da imagem.

3.2. Violação da imagem sem captação real: *deepfake* e avatar não consentido

A utilização indevida de imagens geradas por IA – seja um retrato *deepfake* de alguém em situação vexatória, seja a inserção não autorizada do rosto alheio em conteúdo qualquer – enseja a responsabilidade civil dos envolvidos. No direito brasileiro, em regra, a responsabilidade civil subjetiva exige comprovação de culpa ou dolo do agente (art. 186 c/c 927, caput, do CC). Entretanto, certas situações configuram responsabilidade objetiva, seja por determinação legal expressa, seja pela natureza da ofensa a direitos da personalidade, em que o dano é presumido. No caso do uso não consentido da imagem, a jurisprudência do STJ firmou entendimento de que se trata de hipótese em que a

responsabilidade tende a ser objetiva, principalmente quando há fins econômicos/comerciais na exploração da imagem alheia.[20]

Uma das súmulas do STJ mais relevantes aqui é a Súmula 403, cujo enunciado estabelece: "*Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais.*". Em outras palavras, se alguém obtém proveito econômico ao usar, sem permissão, a imagem ou semelhança de outra pessoa (por exemplo, em propaganda, mercadoria ou conteúdo monetizado), presume-se o dano moral, dispensando a vítima de demonstrar prejuízo específico.

Esse entendimento já foi aplicado em diversos casos. Um exemplo notável é o referido REsp 1.322.704/SP, no qual a atriz Deborah Secco pleiteou indenização pela republicação de suas fotos em revista, alegando extrapolação do contrato de imagem. Embora seu recurso tenha sido negado por questão contratual, o STJ reafirmou que o direito à indenização por uso não autorizado da imagem independe de prova de uso vexatório, bastando o proveito econômico pelo explorador.

> DIREITO CIVIL. DIREITO DE IMAGEM VS DIREITO AUTORAL. ENSAIO FOTOGRÁFICO. VIOLAÇÃO A ARTIGO DA LEI DE DIREITOS AUTORAIS . DESCABIMENTO. DIREITOS DA PERSONALIDADE. EXPLORAÇÃO. CESSÃO . DIREITO DE IMAGEM. ALCANCE CONTRATUAL. INCIDÊNCIA DA SÚMULA N. 5/STJ . 1. O ordenamento jurídico brasileiro, de forma ampla e genérica, confere à fotografia proteção própria de direito autoral. Art. 7º, inciso VII, da Lei n . 9.610/1998 e art. 2 da Convenção de Berna. 2 . Porém, em se tratando de fotografia, para efeitos de proteção do direito autoral das obras artísticas, é autor o fotógrafo e não o fotografado, este último titular de outros direitos da personalidade, como a imagem, a honra e a intimidade. É o fotógrafo o detentor da técnica e da inspiração, quem coordena os demais elementos complementares ao retrato do objeto - como iluminação -, é quem capta a oportunidade do momento e o transforma em criação intelectual, digna, portanto, de tutela como manifestação de cunho artístico. 3. A modelo fotografada não goza de proteção do direito autoral, porque nada cria, dela não emana nenhuma criação do espírito exteriorizada como obra artística . Sua imagem compõe obra artística de terceiros. Portanto, descabe analisar a apontada ofensa ao art. 4º da Lei de Direitos Autorais, uma vez que tal dispositivo não socorre à modelo fotografada, a qual não é titular de direitos

[20] SUPERIOR TRIBUNAL DE JUSTIÇA. Quarta Turma nega à atriz Deborah Secco pedido de danos morais contra Editora Abril. Brasília: STJ, 28 out. 2014. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2014/2014-10-28_17-55_Quarta-Turma-nega-a-atriz-Deborah-Secco-pedido-de-danos-morais-contra-Editora-Abril.aspx

> autorais oponíveis contra a editora da revista na qual as fotos foram divulgadas. 4 . Dissídio jurisprudencial não demonstrado. Casos confrontados que não guardam similitude fática nem merecem soluções jurídicas idênticas. A ideia de que a cessão de direitos de imagem não deve ser interpretada ampliativamente está, a rigor, correta (Arts. 11 e 20 do Código Civil de 2002) . Isso, todavia, não afasta métodos também consagrados de hermenêutica contratual que incidiriam no caso em apreço, como aquele segundo o qual "nas declarações de vontade se atenderá mais à sua intenção que ao sentido literal da linguagem" (art. 85 do CC/1916 e art. 112 do CC/2002); o de que os negócios jurídicos devem ser interpretados conforme os usos e costumes (art. 113, CC/2002); ou que "o silêncio importa anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa" (art . 111 do CC/2002). 5. Com efeito, a solução buscada pela recorrente encontra óbice intransponível na Súmula 5/STJ, pois demandaria reexame de cláusulas contratuais, cláusulas essas cujo alcance - sobretudo em um cenário de dúvida, como amiúde ocorre - não se limita à mera releitura de sua literalidade incontroversa. 6 . Recurso especial parcialmente conhecido e não provido.
>
> (STJ - REsp: 1322704 SP 2012/0092034-4, Relator.: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 23/10/2014, T4 - QUARTA TURMA, Data de Publicação: DJe 19/12/2014 RT vol. 954 p. 484)

Ou seja, havendo utilização mercantil da imagem sem consentimento, configura-se ato ilícito de natureza objetiva – o dever de indenizar surge do próprio fato da violação do direito de imagem, associado ao lucro obtido, sem necessidade de perquirir a intenção ou culpa do agente.

Mas e quando a *deepfake* ou imagem artificial não tem intuito comercial, e sim causa outros danos (como difamação ou abalo emocional)? Nesses casos, a responsabilidade continua existindo, embora recaia na categoria subjetiva tradicional (exigindo dolo ou culpa), já que não há presunção automática do dano como na exploração econômica. Na prática, porém, é comum que o conteúdo manipulado cause dano moral in re ipsa se violar a honra, a privacidade ou acarretar sofrimento à vítima – por exemplo, deepfakes pornográficas envolvendo a face de mulheres (um tipo de abuso infelizmente frequente). Nessas hipóteses, os tribunais tendem a reconhecer o dano moral pelo próprio fato da gravidade da ofensa, ainda que tecnicamente enquadrado na responsabilidade subjetiva. Afinal, produzir e divulgar um vídeo falso, imputando a alguém atos ou falas indecorosas, configura dolo ou, no mínimo, negligência grave, e o prejuízo à dignidade da pessoa é ínsito ao ato ilícito. Decisões do STJ já reconheceram que o fotografado tem direito à imagem cuja violação gera indenização mesmo sem uso vexatório, desde que haja proveito econômico ou ofensa moral.

É importante destacar, ademais, que a responsabilidade civil por violação da imagem possui caráter típico de tutela de direitos da personalidade, o que implica inversão do ônus probatório em certa medida. A simples veiculação não autorizada já configura o ilícito; caberia ao réu, em tese, tentar demonstrar alguma excludente (por exemplo, consentimento do autor da imagem, ou que a situação se enquadra em permissivo legal de ordem pública). Contudo, excludentes são raras nesses casos. Quando muito, poder-se-ia discutir ausência de ilicitude se a imagem foi claramente manipulada em contexto de sátira ou arte (tema que abordaremos na Seção 3.5), mas mesmo aí não há um salvo-conduto absoluto – dependerá da ponderação entre direitos em conflito.

No que tange à jurisprudência dos tribunais superiores, embora ainda não haja muitos precedentes específicos sobre deepfakes, há decisões paradigmáticas sobre uso indevido da imagem. O Supremo Tribunal Federal ("STF"), por seu turno, já ressaltou em julgados que o direito à imagem é resguardado constitucionalmente e sua violação gera dever de indenizar. Por exemplo, no julgamento do RE 1.010.606/RJ (caso do "direito ao esquecimento", 2021), o STF reafirmou que, não obstante ter negado um "direito ao esquecimento" genérico, as lesões concretas a direitos da personalidade (honra, imagem, vida privada) continuam plenamente indenizáveis caso a caso, conforme os mecanismos do direito civil. Em suma, a Corte reconhece que o uso não consentido ou abusivo da imagem de alguém, especialmente se acarretar difusão de fato inverídico ou ofensivo, constitui abuso de direito passível de reparação civil – sem prejuízo de eventuais tutelas específicas, como direito de resposta ou remoção de conteúdo, conforme cada situação.

Por fim, cabe mencionar a possibilidade de responsabilidade objetiva com base no risco ou na lei em contextos de novas tecnologias. Embora hoje não haja no Brasil lei específica atribuindo responsabilidade objetiva ao autor de deepfakes, a doutrina sugere analogias. Alguns autores invocam, por exemplo, o art. 927, parágrafo único, do CC (atividades de risco) para sustentar que quem se utiliza de algoritmos de IA capazes de causar dano grave a terceiros poderia responder independentemente de culpa, dada a periculosidade da atividade. Se uma empresa ou indivíduo deliberadamente opera um sistema de criação de imagens falsas de terceiros, disseminando-as em massa, tal prática pode ser vista como atividade de alto risco à imagem e honra alheias, justificando o dever de reparar objetivamente. Essa construção ainda carece de consolidação jurisprudencial, mas demonstra a tendência de se buscar soluções eficazes. Na prática, contudo, a maior

parte dos casos de *deepfake* tem sido enquadrada na esfera subjetiva tradicional – punindo-se o agente pela conduta dolosa de falsificação e difusão, com reconhecimento de danos morais presumidos pela gravidade (o que, de todo modo, dispensa longas digressões probatórias sobre o abalo sofrido). Em conclusão, seja pela via objetiva (quando houver proveito econômico ou risco excepcional) seja pela subjetiva (nos demais casos), o ordenamento oferece instrumentos para responsabilizar quem utiliza indevidamente imagens artificiais de outra pessoa, garantindo à vítima o direito à indenização por prejuízos materiais e, principalmente, morais.

3.3. Cadeia de responsabilidade: usuário, plataforma e desenvolvedor

A problemática dos deepfakes envolve múltiplos atores, exigindo a análise da cadeia de responsabilidade: quem cria e divulga o conteúdo (usuário), quem provê os meios de circulação (plataformas online) e quem desenvolve a tecnologia algorítmica subjacente (programadores/empresas de IA). O marco normativo brasileiro já possui regras para alguns desses elos – notadamente o Marco Civil da Internet (Lei 12.965/2014 – "MCI") e a LGPD – mas apresenta lacunas quanto a outros, como a responsabilização direta de desenvolvedores de IA. A seguir, examinamos cada componente da cadeia.

A princípio, a pessoa que efetivamente cria o conteúdo ilícito (ex.: monta um vídeo *deepfake* difamatório) ou aquele que o divulga de forma consciente responde primariamente pelos danos causados. Trata-se da aplicação direta dos arts. 186 e 927 do CC: quem, por ação ou omissão voluntária, violar direito e causar dano a outrem comete ato ilícito e deve reparação. No caso, ao fabricar a falsa imagem de alguém ou propagar tal conteúdo sem verificar veracidade, o usuário incorre em culpa ou dolo. Além da responsabilização civil, pode haver responsabilidade penal em certos cenários – por exemplo, se o *deepfake* configura calúnia, difamação, injúria ou mesmo divulgação de pornografia não consensual (crimes previstos no Código Penal). Aqui, não há grande novidade: é a imputação direta ao agente causador. O maior desafio em relação ao usuário infrator, como veremos na seção 3.4, é identificá-lo e vinculá-lo ao conteúdo, dada a facilidade de anonimato na internet e à disseminação rápida. Porém, uma vez identificado, ele arcará com os danos morais e materiais sofridos pela vítima, em regime subjetivo (pois se exige a demonstração de sua conduta culposa ou dolosa, o que normalmente está presente).

No que tange aos intermediários (como Facebook/Instagram, YouTube, TikTok, sites etc.), a regra-matriz é dada pelo MCI, que adotou no Brasil um sistema de responsabilidade condicionada (safe harbor) para provedores de aplicações de internet em relação a conteúdos de terceiros. Conforme o art. 19 do MCI, as plataformas só respondem civilmente por danos decorrentes de conteúdo gerado por usuários se, após ordem judicial específica, não tomarem as providências para remover o conteúdo ilícito. Em outras palavras, não há dever geral de monitoramento ou filtro prévio; porém, uma vez notificado judicialmente de que determinado vídeo/foto é ilegal (por exemplo, um *deepfake* violador do direito de imagem), o provedor deve removê-lo, sob pena de se tornar solidariamente responsável pelos danos causados a partir daquele momento. Essa disciplina foi pensada exatamente para equilibrar a liberdade na internet e a proteção a direitos individuais. No caso de deepfakes ofensivos, significa que a vítima normalmente precisará acionar a Justiça para obrigar a plataforma a retirar o material, salvo em situações excepcionais previstas em lei. (MEDON, 2021)

Uma exceção importante no MCI diz respeito a imagens de nudez ou de caráter sexual privado divulgadas sem consentimento. O art. 21 do MCI (introduzido pela Lei 13.718/2018) prevê que, havendo divulgação não autorizada de "imagens, vídeos ou outros materiais contendo cena de nudez ou ato sexual de caráter privado" de alguém, o provedor de aplicações deve remover esse conteúdo mediante simples notificação do interessado, dispensando ordem judicial. Caso não remova, pode ser responsabilizado civilmente pelos danos resultantes.

Esta regra foi criada para agilizar a retirada de conteúdos de *revenge porn* e assemelhados. Aplica-se aqui um entendimento de que eventuais *deepfakes* pornográficos – em que o rosto da vítima é inserido em cenas de sexo ou nudez – se enquadram na proteção do art. 21, mesmo que a imagem tenha sido artificialmente criada, pois o material veiculado contém cena sexual de caráter privado atribuída indevidamente à vítima. Assim, uma mulher cuja face foi usada em um vídeo pornográfico falso poderia notificar diretamente a plataforma, que terá o dever legal de agir prontamente para remover o vídeo sob pena de responder pelos danos da manutenção.

Em suma, o MCI atribui às plataformas um papel reativo: não respondem por todo e qualquer *deepfake* postado, mas têm a obrigação de agir ao serem cientificadas da ilicitude – seja via ordem judicial (regra geral do art. 19) ou via notificação extrajudicial da vítima em caso de intimidade violada (regra especial do art. 21).

Em complemento, convém mencionar que novas regulamentações estão surgindo para ampliar a responsabilidade das plataformas quanto a conteúdos sintéticos. O Tribunal Superior Eleitoral ("TSE"), por exemplo, editou normas específicas para eleições: a Resolução TSE 23.610/2019, alterada pela Res. 23.732/2024,[21] proibiu expressamente o uso de deepfakes para difundir fatos inverídicos em campanhas, prevendo sanções severas. Segundo o art. 9º-C dessa norma, é vedado o uso de conteúdo manipulado (*deepfake*) para criar ou alterar a imagem ou voz de pessoas (vivas, mortas ou fictícias) com intenção de prejudicar ou favorecer candidatos. O descumprimento caracteriza abuso de poder e pode levar à cassação do registro ou mandato. Embora essa regulamentação seja própria do âmbito eleitoral, ela impõe às plataformas e aos candidatos obrigações adicionais de vigilância nesse contexto específico. Fora do período eleitoral, discute-se no Congresso o chamado "PL das Fake News" (PL 2630/2020), que pretende exigir que plataformas rotulem conteúdos sintéticos e respondam mais ativamente por desinformação, inclusive deepfakes. Até o presente ano de 2025, tal legislação está em debate, mas reflete uma tendência de aumentar a responsabilização das plataformas – hoje relativamente limitada pelo regime do MCI – diante dos perigos da IAG.

Por outro lado, talvez o ponto mais inovador e ainda carente de disciplina clara seja referente aos desenvolvedores de IA e fornecedores das tecnologias. A LGPD traz obrigações a agentes de tratamento de dados pessoais, o que pode incluir desenvolvedores de aplicações de IA que lidam com dados dos usuários, mas não foi concebida especificamente para deepfakes. No contexto dos deepfakes, podemos pensar em desenvolvedores de dois tipos: (a) aqueles que criam os algoritmos ou softwares capazes de gerar deepfakes (por exemplo, a empresa que desenvolveu um aplicativo de face-swap ou um modelo de síntese de voz); e (b) aqueles que treinam IA utilizando dados pessoais alheios (por exemplo, alimentando um sistema com milhares de fotos de figuras públicas sem consentimento para criar avatares realistas).

Atualmente, não existe no Brasil uma lei que atribua diretamente responsabilidade civil objetiva aos desenvolvedores pelo mau uso de suas ferramentas por terceiros. Em geral, se a ferramenta em si não é ilícita (pois pode ter usos legítimos, como em

[21] MIGALHAS. Justiça Eleitoral suspende perfil do Instagram por uso de deepfake. Migalhas, 27 maio 2024. Disponível em: https://www.migalhas.com.br/quentes/408157/justica-eleitoral-suspende-perfil-de-instagram-por-uso-de-deepfake.

entretenimento ou acessibilidade), o seu criador não responde automaticamente por cada uso abusivo feito por usuários. Contudo, a doutrina e especialistas em proteção de dados apontam a necessidade de estabelecer deveres de segurança e mitigação de riscos também para os desenvolvedores. Bruno Bioni – um dos expoentes na área de proteção de dados – , em entrevista à Folha de S. Paulo, alerta que a regulação de IA é necessária "a*té mesmo para gerar algum tipo de obrigação aos desenvolvedores da IA*", dado que esses modelos trazem riscos significativos, desde fraudes cibernéticas até "*produção de nudes indevidos*" com rostos de mulheres.[22] Defendeu que "*novos riscos exigem novas técnicas, novos direitos e deveres*", ou seja, é preciso impor novas regulações e políticas públicas que criem responsabilidade para quem projeta e disponibiliza essas tecnologias. Isso poderia incluir, por exemplo, obrigações de implementar filtros antiabusos, marcas d'água digitais para indicar que certo conteúdo é sintético, ou responder solidariamente se a ferramenta for deliberadamente voltada a atos ilícitos.

No âmbito da LGPD, se o processo de criação da *deepfake* envolver tratamento de dados pessoais (e geralmente envolve, pois a imagem de um rosto real é dado pessoal biométrico), pode-se responsabilizar o controlador desses dados. Suponha que um desenvolvedor mantenha um aplicativo online em que usuários enviem fotos de terceiros para gerar montagens: essa empresa desenvolvedora passa a tratar dados pessoais sensíveis e deve observar bases legais, princípios e medidas de segurança. Usar ou permitir o uso de dados pessoais sem consentimento ou outra base legal pode configurar infração à LGPD, sujeitando o desenvolvedor a sanções administrativas e também a reparar danos causados aos titulares (art. 42 da LGPD). Inclusive, a LGPD adota a responsabilidade objetiva dos agentes de tratamento em caso de danos decorrentes de violação da lei, com inversão do ônus da prova a favor do titular dos dados, cabendo ao controlador demonstrar que observou a legislação (art. 42, §2º). Desse modo, se um software de IA for responsável pelo vazamento ou uso indevido de imagens pessoais, a empresa por trás pode ser civilmente responsabilizada, ainda que não haja dolo.

No caso específico de deepfakes, a aplicação da LGPD é inovadora: poderíamos ter, por exemplo, uma ação de uma vítima alegando que sua imagem (dado pessoal) foi tratada de forma ilícita por certo sistema de IA, causando-lhe danos – caberia então ao

[22] FOLHA DE S. PAULO. Nudes feitos com IA geram novos riscos para mulheres e esbarram em falta de regulação. Folha de S.Paulo, São Paulo, 11 nov. 2023. Disponível em: https://www1.folha.uol.com.br/cotidiano/2023/11/nudes-feitos-com-ia-geram-novos-riscos-para-mulheres-e-esbarram-em-falta-de-regulacao.shtml

controlador (desenvolvedor) provar que tomou precauções ou que não tinha como evitar o mau uso. Essa via ainda não foi testada extensivamente nos tribunais, mas é um caminho possível para responsabilizar os fornecedores da tecnologia sob a ótica da proteção de dados pessoais.

Por ora, no entanto, a responsabilização de desenvolvedores ocorre mais no campo moral e regulatório do que judicial. Há um consenso emergente de que ética na IA exige que fabricantes incorporem salvaguardas e respondam por falhas previsíveis. Por exemplo, se uma empresa treina um modelo generativo usando indevidamente imagens colhidas da internet sem autorização (violando direitos de imagem e talvez direito autoral alheio), ela pode ser acionada por esses titulares pela violação de seus direitos, ainda que a empresa não tenha ela mesma divulgado deepfakes. Já sob a perspectiva do direito do consumidor, se um desenvolvedor comercializa um aplicativo alegando ser seguro ou lícito e usuários o empregam para atos ilegais, poder-se-ia discutir a responsabilidade por defeito do produto ou falta de adequação (art. 12 do CDC), embora isso dependa de se caracterizar o software como produto defeituoso – o que não é trivial se o "defeito" advém do uso intencionalmente mau pelo usuário.

Em síntese, a cadeia de responsabilidade hoje se estrutura assim: o usuário infrator é o primeiro responsável; as plataformas respondem subsidiariamente, caso não cooperem após notificadas (conforme MCI, art. 19) ou, em situações de intimidade, imediatamente quando notificadas (MCI, art. 21); e os desenvolvedores de IA, por sua vez, ainda carecem de regras específicas, mas há forte tendência doutrinária e regulatória de envolvê-los na responsabilização, seja via futuras leis de IA, seja pela aplicação criativa de normas existentes (LGPD, CDC, etc.) para obrigá-los a prevenir e mitigar os danos das deepfakes.

3.4. Dificuldades Probatórias e Tutela Inibitória na Manipulação Algorítmica da Imagem

A emergência das deepfakes traz não apenas questões de direito material, mas também desafios de ordem processual. Dois aspectos merecem destaque: as dificuldades probatórias envolvidas em demonstrar a falsificação e a autoria do conteúdo, e a busca

por tutelas inibitórias (preventivas) eficazes para evitar ou estancar danos muitas vezes irreparáveis à imagem da vítima.

Identificar e provar que determinada imagem ou vídeo é uma *deepfake* pode ser tecnicamente complexo. As versões mais sofisticadas dessa tecnologia produzem conteúdos de alta verossimilhança, de modo que um leigo pode ter dificuldade em discernir o real do manipulado.[23] Para convencer o Judiciário de que, por exemplo, um vídeo atribuído a alguém é falso, a parte lesada frequentemente precisa lançar mão de perícias técnicas digitais. Especialistas forenses podem analisar metadados, detectar artefatos digitais (como inconsistências em pixels, iluminação ou sincronização labial) ou utilizar softwares que identificam marcas sutis deixadas pelos algoritmos (*deepfake detection*). Todavia, esses procedimentos demandam tempo e recursos, o que é problemático diante da rapidez com que deepfakes podem viralizar.

Além de provar a falsidade do conteúdo, há a questão de atribuir responsabilidade a alguém. Os criadores e disseminadores de deepfakes costumam esconder sua identidade atrás de perfis falsos, redes onion ou simplesmente postando anonimamente em fóruns e grupos. Rastreá-los envolve pedidos a provedores de internet para fornecimento de registros de IP, logs de acesso e outros dados – o que pode esbarrar em limites jurisdicionais (se o responsável estiver no exterior) ou mesmo em dificuldades técnicas (VPNs, redes anônimas). Como nota Medon (2021), nos Estados Unidos já se apontou que a dificuldade em rastrear o criador/distribuidor da *deepfake* pode deixar a vítima sem opção a não ser acionar a plataforma onde o vídeo circula, visto que os autores materiais muitas vezes fogem da jurisdição ou permanecem desconhecidos. Esse cenário certamente se reflete no Brasil: em muitos casos práticos, a pessoa lesada consegue, no máximo, que se derrube o conteúdo via ordem judicial à rede social (como discutido na seção anterior), mas punir civilmente o autor original pode se tornar inviável se ele não for identificado ou estiver fora do alcance.

Há ainda a possibilidade de o réu (quando identificado) alegar que não houve adulteração – invertendo a acusação, poderia afirmar que o vídeo é real. Isso inauguraria uma "batalha de perícias" para comprovar a verdade. Imaginemos uma situação-limite:

[23] DONEDA, Danilo; ALMEIDA, Virgílio; LEMOS, Ronaldo. Com avanço tecnológico, fake news vão entrar em fase nova e preocupante. Disponível em: https://doneda.net/com-avanco-tecnologico-fake-news-vao-entrar-em-fase-nova-e-preocupante/#:~:text=deep%20fake%20news,relat%C3%B3rio%20do%20Conselho%20da%20Europa

um vídeo aparece mostrando uma figura pública em ato comprometedor; ela alega ser *deepfake*, mas quem divulgou insiste que é verdadeiro. O ônus recairia sobre quem alega a falsidade (a vítima) de demonstrá-la. Esse tipo de controvérsia probatória é inédito até então e exigirá do Judiciário adaptação e entendimento básico de tecnologias de edição de mídia. Ferramentas de autenticação digital, como hashes ou assinaturas em fotos/vídeos originais, poderão ganhar relevância para atestar autenticidade, embora na prática poucas pessoas usem esses recursos em seus conteúdos pessoais.

Dada a dificuldade de "desfazer" o estrago após uma *deepfake* difamatória se espalhar, é crucial manejar mecanismos de tutela antecipada ou inibitória para cessar a divulgação o quanto antes. O direito brasileiro prevê, no art. 12 do CC, que a vítima de ameaça ou lesão a direito da personalidade (como a imagem) pode requerer providências judiciais adequadas para impedir a consumação ou fazer cessar a violação, independentemente de outras sanções. Na prática, isso se traduz em medidas liminares para retirada de conteúdo, bloqueio de perfis ou proibição de novas publicações, muitas vezes concedidas inaudita altera parte (sem ouvir o outro lado inicialmente), dado o perigo de demora.

Os tribunais têm se mostrado receptivos a tais pleitos diante de deepfakes. Por exemplo, na esfera eleitoral – onde a rapidez é fundamental – já houve decisões ordenando imediata remoção de vídeos e suspensão de contas que divulgaram deepfakes contra candidatos, com fixação de multa diária em caso de descumprimento.[24] Em um caso de 2024, um juiz eleitoral em Pernambuco determinou liminarmente a suspensão de um perfil do Instagram que postou um vídeo *deepfake* do jornalista William Bonner difamando políticos locais, e ainda impôs multa diária de R$1.000,00 se o responsável não cumprisse, além de oficiar a plataforma para fornecer os dados do infrator. Embora esse exemplo seja do âmbito eleitoral, ele ilustra o modelo de tutela inibitória que também se aplica no cível.

Um desafio, contudo, é que a internet é difusa e o conteúdo pode reaparecer em outras páginas ou ser republicado por terceiros. Assim, uma tutela efetiva precisa muitas vezes ser ampla, ordenando não só a remoção pontual, mas também proibindo o réu de recolocar a *deepfake* ou publicar em quaisquer outros meios sob pena de multa ou outras

[24] MIGALHAS. Justiça Eleitoral suspende perfil do Instagram por uso de deepfake. Migalhas, 27 maio 2024. Disponível em: https://www.migalhas.com.br/quentes/408157/justica-eleitoral-suspende-perfil-de-instagram-por-uso-de-deepfake

medidas. Em certos casos extremos, pode-se cogitar ordem judicial às operadoras de internet para bloquear completamente o acesso a um determinado *link* ou site que esteja hospedando o conteúdo ilícito, caso a plataforma originária não colabore (o que tangencia debates sobre neutralidade de rede e censura, devendo ser usado com cautela).

A tutela inibitória também se mostra na concessão de direito de resposta ou esclarecimento, quando aplicável. Embora mais comum em contexto de imprensa, nada impede que um juiz, ao analisar uma *deepfake* difamatória, determine que o responsável publique uma retratação ou esclareça que se tratava de conteúdo falso, visando mitigar o impacto na reputação da vítima.

Quanto às dificuldades probatórias ligadas à tutela de urgência, felizmente o padrão para concessão de liminar é a prova sumária da verossimilhança. Ou seja, a vítima não precisa provar de forma exauriente que o vídeo é falso; basta demonstrar indícios plausíveis da adulteração e o risco iminente de dano. Por exemplo, se a pessoa nunca esteve no local ou contexto exibido no vídeo, ou se peritos preliminarmente apontam incoerências técnicas, isso já pode embasar a decisão provisória. A tendência, portanto, é que o Judiciário adote uma postura protetiva diante de indícios de *deepfake*, concedendo a retirada urgente "*ut res magis valeat quam pereat*" (para que o direito da personalidade não pereça ante a demora). Depois, no mérito da ação, aprofunda-se a prova pericial para fins de indenização, mas ao menos o conteúdo já terá sido sustado a tempo.

Outro ponto a considerar é a cooperação internacional e interplataformas. Um usuário mal-intencionado pode, após ter conteúdo removido e perfil banido em uma rede social, migrar para outra ou para sites estrangeiros para continuar a divulgação. Nesses casos, a efetividade das decisões nacionais esbarra em questões de jurisdição e competência. A vítima e seus advogados devem perseguir a remoção em todos os locais onde a *deepfake* surja, o que é oneroso. Uma solução incipiente tem sido conversar com as próprias plataformas, que desenvolvem políticas internas contra deepfakes (por exemplo, o Facebook e o Twitter anunciaram diretrizes para remover mídias sintéticas que induzam erro grave). Contudo, essas políticas às vezes exigem que se prove a falsidade, recaindo novamente no problema probatório.

Por fim, vale mencionar a utilidade de tutelas antecipatórias de produção de prova – como conseguir logs de acesso, endereços IP, dados cadastrais – ainda na fase inicial, para permitir identificar os autores. MCI obriga provedores a guardarem certos registros

e franquear ao juiz o acesso a eles mediante ordem (art. 22). Assim, parte da estratégia processual contra deepfakes é primeiro identificar o responsável e a extensão da divulgação, para então calibrar as medidas inibitórias e os pedidos indenizatórios. Essa etapa, infelizmente, encontra a barreira já citada: se o criador usou meios de anonimato robustos, nem mesmo os registros de provedores locais ajudarão.

Em suma, no terreno probatório, as deepfakes demandam aperfeiçoamento pericial e cooperação técnica, enquanto no terreno da tutela jurisdicional requerem agilidade e abrangência para conter danos de difícil reparação. Os juristas brasileiros têm enfatizado que o poder geral de cautela dos juízes e as ações inibitórias devem ser amplamente empregados aqui, sob pena de o direito à imagem se tornar "inefetivo" diante da rapidez e impacto das manipulações algorítmicas. Esse enfoque preventivo é coerente, inclusive, com a ideia de que direitos de personalidade têm caráter absoluto e extrapatrimonial, merecendo barreiras contra a simples prospectividade de sua violação (evitar o dano antes que ocorra ou se agrave, ao invés de apenas indenizar depois). A tutela inibitória, portanto, é peça-chave no arsenal contra os malefícios das deepfakes, complementando a reparação civil tradicional com uma resposta mais célere e orientada a resguardar a dignidade da pessoa em ambiente digital.

3.5. Colisão entre imagem, liberdade de expressão e interesse público

A interação entre deepfakes e direito à imagem não pode ser analisada isoladamente dos princípios constitucionais, em especial da liberdade de expressão (CF, art. 5º, IV e IX; art. 220). Frequentemente, casos envolvendo imagens manipuladas situam-se em uma zona cinzenta onde a proteção da personalidade individual colide com interesses de liberdade artística, humorística ou informativa. É necessário, portanto, entender como o ordenamento equilibra o direito à imagem – intimamente ligado à honra, privacidade e identidade da pessoa – e o direito de se expressar, criar sátiras, paródias e obras artísticas que, por vezes, se valem da imagem de figuras reais.

A princípio, ambos os direitos têm assento constitucional: de um lado, o direito à imagem, honra e vida privada (art. 5º, X, CF) é inviolável, assegurando indenização pelo dano material ou moral decorrente de sua violação; de outro, a livre manifestação do pensamento, criação, expressão e informação (arts. 5º IV e IX, e art. 220, CF) é garantida, vedada qualquer censura prévia de natureza política, ideológica e artística. Nenhum

desses direitos é absoluto – havendo conflito, cabe ao intérprete ponderar os valores em jogo conforme a situação concreta, buscando minimizar restrições a cada um (princípio da concordância prática).

No contexto das deepfakes, tal colisão assume contornos peculiares: se a montagem digital for utilizada para fins de sátira ou paródia, sem intenção de fraude ou difamação, poderemos ter um caso de exercício legítimo da liberdade criativa. Por exemplo, uma paródia política em formato de vídeo *deepfake* (claramente humorística, exagerada, sem pretensão de ser entendida como real) pode ser equiparada às tradicionais caricaturas ou charges feitas por desenhistas, que são culturalmente aceitas e juridicamente protegidas como crítica social. O STF já teve oportunidade de se manifestar a favor do humor, ao julgar inconstitucional a antiga proibição legal de piadas com candidatos durante o período eleitoral. Na ADI 4.451/DF, em 2010, a Corte entendeu, por unanimidade, que vedar sátiras a candidatos violava a liberdade de expressão e o direito à crítica bem-humorada no processo político, ressaltando que o humor é uma forma válida de manifestação do pensamento na democracia, mesmo em período eleitoral sensível:

> LIBERDADE DE EXPRESSÃO E PLURALISMO DE IDEIAS. VALORES ESTRUTURANTES DO SISTEMA DEMOCRÁTICO. INCONSTITUCIONALIDADE DE DISPOSITIVOS NORMATIVOS QUE ESTABELECEM PREVIA INGERÊNCIA ESTATAL NO DIREITO DE CRITICAR DURANTE O PROCESSO ELEITORAL. PROTEÇÃO CONSTITUCIONAL AS MANIFESTAÇÕES DE OPINIÕES DOS MEIOS DE COMUNICAÇÃO E A LIBERDADE DE CRIAÇÃO HUMORISTICA . 1. A Democracia não existirá e a livre participação política não florescerá onde a liberdade de expressão for ceifada, pois esta constitui condição essencial ao pluralismo de ideias, que por sua vez é um valor estruturante para o salutar funcionamento do sistema democrático. 2. A livre discussão, a ampla participação política e o princípio democrático estão interligados com a liberdade de expressão, tendo por objeto não somente a proteção de pensamentos e ideias, mas também opiniões, crenças, realização de juízo de valor e críticas a agentes públicos, no sentido de garantir a real participação dos cidadãos na vida coletiva . 3. São inconstitucionais os dispositivos legais que tenham a nítida finalidade de controlar ou mesmo aniquilar a força do pensamento crítico, indispensável ao regime democrático. Impossibilidade de restrição, subordinação ou forçosa adequação programática da liberdade de expressão a mandamentos normativos cerceadores durante o período eleitoral. 4 . Tanto a liberdade de expressão quanto a participação política em uma Democracia representativa somente se fortalecem em um ambiente de total visibilidade e

> possibilidade de exposição crítica das mais variadas opiniões sobre os governantes. 5. O direito fundamental à liberdade de expressão não se direciona somente a proteger as opiniões supostamente verdadeiras, admiráveis ou convencionais, mas também aquelas que são duvidosas, exageradas, condenáveis, satíricas, humorísticas, bem como as não compartilhadas pelas maiorias. Ressalte-se que, mesmo as declarações errôneas, estão sob a guarda dessa garantia constitucional . 6. Ação procedente para declarar a inconstitucionalidade dos incisos II e III (na parte impugnada) do artigo 45 da Lei 9.504/1997, bem como, por arrastamento, dos parágrafos 4º e 5º do referido artigo.
>
> (STF - ADI: 4451 DF, Relator.: ALEXANDRE DE MORAES, Data de Julgamento: 21/06/2018, Tribunal Pleno, Data de Publicação: 06/03/2019)

Esse precedente sinaliza que a mera utilização da imagem de alguém em contexto satírico não autoriza, por si só, a proibição ou sanção, desde que não se converta em ataque pessoal gratuito divorciado de propósito humorístico ou informativo.

No STJ, merece menção o caso do blog "*Falha de S.Paulo*", que parodiava o jornal Folha de S.Paulo. A empresa jornalística acionou os autores da paródia por uso do nome e logotipo similares e por suposta violação da imagem de seus jornalistas e marca. Em 2017, a 4ª Turma do STJ deu ganho de causa aos criadores do blog, reconhecendo expressamente que se tratava de uma paródia e crítica bem-humorada, protegida pela liberdade de expressão. O min. Luis Felipe Salomão, ao abrir a divergência vencedora, afirmou que a paródia – caracterizada pelo deboche, ironia e releitura cômica de obra alheia – é prática admitida e de acordo com o direito à livre expressão, dispensando autorização do titular da obra parodiada.[25] Essa decisão é paradigmática: ainda que envolvesse marca e conteúdo jornalístico, tangencia o uso de imagem de pessoas reais (já que o blog usava elementos visuais do jornal e mencionava jornalistas) e reforça que a sátira gozará de licitude quando for identificável como tal e não enganar o público quanto à identidade ou autenticidade do conteúdo.

Transpondo esses entendimentos para o universo das deepfakes, podemos concluir que há situações em que a criação de um "*deepfake* satírico" ou artístico poderia ser considerada um exercício legítimo de expressão, oponível a uma alegação de violação

[25] MIGALHAS. Blog Falha de S.Paulo não viola direito de marca do matutino Folha de S.Paulo. Migalhas, 21 jun. 2017. Disponível em: https://www.migalhas.com.br/quentes/260772/blog-falha-de-s-paulo-nao-viola-direito-de-marca-do-matutino-folha

de imagem. Suponha-se um vídeo humorístico colocando o rosto de um político em uma cena de filme famoso, para fazer crítica bem-humorada – desde que o contexto deixe claro tratar-se de montagem de humor (por exemplo, publicado em páginas de comédia, com tom obviamente exagerado), dificilmente se poderia considerar ilícito. A imagem do político, embora utilizada sem consentimento, estaria dentro do limite de tolerância imposto a figuras públicas, que devem aceitar maior exposição e críticas, inclusive através de paródias.

Contudo, é fundamental distinguir paródia ou crítica jocosa de ataques difamatórios mascarados de humor. Nem tudo que se alega ser piada estará protegido. Se uma *deepfake* atribui falsamente a alguém um ato criminoso ou falas injuriosas, e o autor tenta alegar que era "sátira", a análise do contexto dirá se um observador médio entenderia aquilo como brincadeira ou como fato. Um vídeo falsificado com intuito de enganar, mesmo que tenha um teor escandaloso, não será considerado paródia legítima se a intenção for difamar ou manipular a opinião alheia. Nesses casos, prevalece o direito da personalidade. A jurisprudência já enfrentou casos de humoristas sendo processados por piadas consideradas ofensivas: por exemplo, o humorista Rafinha Bastos foi condenado a indenizar a cantora Wanessa Camargo por uma piada de extremo mau gosto envolvendo seu bebê, demonstrando que há limites quando a "piada" atinge indevidamente a dignidade alheia.[26] Assim, o humor não é carta branca para violar a imagem/honra; se o conteúdo for manifestamente abusivo ou causar dano desproporcional, pode-se afastar a excludente da liberdade de expressão e responsabilizar o autor.

Entende-se, portanto, que as cortes superiores têm reiterado o conceito de ponderação proporcional. Em síntese: se o uso da imagem contribuir para um debate de interesse público, uma crítica social ou obra artística genuína, a liberdade de expressão tende a prevalecer; por outro lado, se a utilização da imagem for essencialmente para espalhar desinformação, fraudar ou humilhar, o direito à imagem falará mais alto, legitimando sanções e remoções.

No caso específico de *deepfakes*, há um agravante, todavia: a sua potencial capacidade de enganar. Diferentemente de uma caricatura obviamente tosca ou de um texto claramente irônico, um vídeo ultrarrealista pode ser levado a sério por muitos. Isso

[26] JUSBRASIL. Piadas, sátiras e o limite do humor: a proteção jurídica dos comediantes. JusBrasil, 17 mar. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/piadas-saturas-e-o-limite-do-humor-a-protecao-juridica-dos-comediantes/3228223237

faz com que mesmo uma intenção humorística possa ter consequências reais gravosas. Por isso, alguns especialistas sugerem exigências de sinalização clara quando se divulgar uma *deepfake* de paródia (por exemplo, inserindo avisos, marcas d'água, ou contextualmente deixando inequívoco que se trata de montagem). Essa boa prática pode evitar tanto mal-entendidos pelo público quanto eventuais responsabilizações legais. Afinal, se um *deepfake* "artístico" for interpretado como fato por parte do público e causar danos, o seu autor poderá enfrentar ações judiciais e terá que provar que não agiu com imprudência.

CAPÍTULO 4 – Soluções Jurídicas, Responsabilidade Civil e Caminhos para o Futuro

4.1. Dano moral e material pela reprodução sintética da imagem

O uso não autorizado da imagem alheia – ainda que seja por meios artificiais, como deepfakes ou avatares sintéticos – configura violação aos direitos da personalidade e ato ilícito em si mesmo.[27] O STJ, por meio da súmula 403[28] consolidou o entendimento de que a publicação não autorizada da imagem de alguém, para fins econômicos ou comerciais, gera dano moral in re ipsa, isto é, dano moral puro, independentemente de prova de prejuízo concreto. Assim, a simples utilização da imagem (real ou sintetizada) sem consentimento já é passível de reparação moral, dada a ofensa à dignidade e privacidade da pessoa retratada.

Além do dano moral presumido, é possível a cumulação com dano material caso haja exploração econômica da imagem sem autorização. A própria Súmula 403 do STJ tem fundamento no art. 20 do CC, dispositivo que protege o direito à imagem e permite tanto a inibição do uso não consentido quanto a indenização por prejuízos. Com base nesse preceito, vítimas de uso comercial indevido de suas imagens (inclusive *deepfakes* utilizados em campanhas ou publicidade) têm direito à reparação material pelos ganhos

[27] LEX. "Uso indevido de imagem para fins comerciais gera dano moral". Disponível em: https://www.lex.com.br/uso-indevido-de-imagem-para-fins-comerciais-gera-dano-moral/#:~:text=%E2%80%9CO%20uso%20n%C3%A3o%20autorizado%20de,pelo%20artigo%205%C2%BA%2C%20inciso%20X

[28] BRASIL. Superior Tribunal de Justiça. Súmula n. 403, de 27 de agosto de 2009. Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. Disponível em: https://www.stj.jus.br

indevidos obtidos pelo explorador ou pelo valor de licença da sua imagem. A jurisprudência reconhece que o uso não autorizado da imagem gera dano material e moral cumulativamente, sendo ambos indenizáveis na mesma ação[29] (Súmula 37/STJ).

A doutrina civilista corrobora esses entendimentos. Autores enfatizam que o direito à imagem é atributo personalíssimo, protegido constitucionalmente (CF, art. 5º, X) e pelo CC, de maneira irrenunciável e intransmissível. Nelson Rosenvald e Ana Carolina Ferreira de Melo Brito[30], por exemplo, salientam que a imagem integra a cláusula geral de tutela da pessoa humana e não pode ser utilizada por terceiros sem consentimento expresso, salvo exceções legais estritas (como fins jornalísticos de interesse público). Nesse sentido, a utilização de *deepfakes* que reproduzem a fisionomia ou voz de alguém, sem autorização, viola diretamente o núcleo dos direitos de personalidade – devendo o responsável (seja quem criou o conteúdo sintético ou quem o divulgou) ser responsabilizado civilmente pelos danos causados.

Importante notar que a responsabilidade pode recair solidariamente sobre plataformas digitais que difundem conteúdos ilícitos, caso descumpram ordens de remoção. Embora o Marco Civil da Internet (Lei 12.965/2014) adote regime específico de responsabilidade (vide item 4.2), a jurisprudência e a doutrina entendem que grandes plataformas não podem se eximir totalmente: espera-se diligência na contenção de violações evidentes aos direitos de personalidade, de modo que quem detém maior capacidade técnica e aufere lucro com o conteúdo (como as big techs) deve assumir um

[29] RECURSO INOMINADO. AÇÃO DE OBRIGAÇÃO DE FAZER C/C PEDIDO DE INDENIZAÇÃO POR DANOS MORAIS E MATERIAIS. UTILIZAÇÃO INDEVIDA DE FOTOGRAFIA. SENTENÇA DE PARCIAL PROCEDÊNCIA. ALEGAÇÃO DE QUE MERAMENTE REPRODUZIU FOTOGRAFIA AMPLAMENTE PUBLICADA E DISSEMINADA NA INTERNET – IRRELEVÂNCIA – RESPONSABILIDADE CIVIL DA RECLAMADA PELA VIOLAÇÃO DE DIREITO AUTORAL – ARTIGO 24 DA LEI Nº 9.810/1998 – USO INDEVIDO DE IMAGEM SEM ANUÊNCIA DO AUTOR E SEM CONTRAPRESTAÇÃO – DANO MORAL QUE INDEPENDE DE PROVA – APLICAÇÃO DA SÚMULA 403 DO STJ – DANOS MORAIS VERIFICADOS. SENTENÇA MANTIDA POR SEUS PRÓPRIOS FUNDAMENTOS. RECURSO INOMINDO DESPROVIDO.1. "Súmula 403/STJ – Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais".2. "A simples publicação de fotografias, sem indicação da autoria, como se fossem obra artística de outrem, é suficiente à caracterização do dano moral e a proteção dos direitos autorais sobre fotografias está expressamente assegurada, nos termos do inciso VII, do art. 7º, da Lei 9.610/98" (STJ, 4ª T., AgInt no REsp 1.457.774/PR, Rel. Ministro LUIS FELIPE SALOMÃO, j. 19.09.2017, DJe 25.09.2017) (TJPR - 5ª Turma Recursal dos Juizados Especiais - 0023665-02.2019.8.16.0182 - Curitiba - Rel.: JUÍZA DE DIREITO SUBSTITUTO EM SEGUNDO GRAU MARIA ROSELI GUIESSMANN - J. 09.09.2020)

[30] CANHADAS FILHO, Gilberto; BRITO, Ana Carolina Ferreira de Melo. A inteligência artificial e os limites no uso do direito de imagem. Migalhas, 18 jul. 2023. Disponível em: https://www.migalhas.com.br/depeso/390067/a-inteligencia-artificial-e-os-limites-no-uso-do-direito-de-imagem

ônus maior na prevenção de danos.[31] Em suma, no uso não autorizado de imagens (reais ou sintéticas) há um consenso jurídico: violou, indenizou – assegurando-se reparação integral por danos morais e materiais.

4.2. Tutela preventiva e inibitória (art. 12 CC e art. 497 CPC) e remoção de conteúdo no MCI

Diante da rápida propagação de deepfakes e outros conteúdos lesivos na internet, ganha relevo a tutela preventiva dos direitos da personalidade. O CC, em seu art. 12,[32] permite ao titular exigir que cesse a ameaça ou lesão a direito de personalidade, independentemente de pedido indenizatório. Trata-se de base legal para ordens judiciais de remoção e abstenção, visando evitar ou estancar danos futuros à honra, imagem, intimidade etc. Já o CPC, no art. 497,[33] complementa esse mecanismo ao prever a tutela específica das obrigações de fazer ou não fazer, incluindo a chamada tutela inibitória (parágrafo único do art. 497) para prevenir a prática, continuação ou repetição de atos ilícitos. Em suma, o ordenamento oferece ao lesado instrumentos para inibir proativamente violações de direitos de personalidade, sem necessidade de esperar a consumação do dano.

A tutela inibitória caracteriza-se por não exigir prova de dano efetivo – basta a demonstração do ato ilícito ou da probabilidade de sua ocorrência para justificar a intervenção do juiz. Como ensina o ilustre professor Luiz Guilherme Marinoni, a "*ação inibitória se volta contra a possibilidade do ilícito, ainda que se trate de repetição ou continuação"* ou seja, "*é voltada para o futuro, e não para o passado*" e, portanto, "*não requer nem mesmo a probabilidade do dano, contentando-se com a simples probabilidade de ilícito*".[34] Ou seja, seria possível obter, por exemplo, uma ordem judicial

[31] REIS, Francisca Sílvia da Silva. Deepfakes e práticas de consumo: integridade informacional, proteção de dados e direitos de personalidade na ordem econômica digital. Revista FT (Sistemas de Informação, v. 29, ed. 150/SET 2025). Disponível em: https://revistaft.com.br/deepfakes-e-praticas-de-consumo-integridade-informacional-protecao-de-dados-e-direitos-de-personalidade-na-ordem-economica-digital/

[32] BRASIL. Código Civil. Lei n. 10.406, de 10 de janeiro de 2002. Diário Oficial da União: Brasília, DF, 11 jan. 2002. Art. 12.

[33] BRASIL. Código de Processo Civil. Lei n. 13.105, de 16 de março de 2015. Diário Oficial da União: Brasília, DF, 17 mar. 2015. Art. 497.

[34] MARINONI, Luiz Guilherme. Tutela inibitória e tutela de remoção do ilícito. 2004. Disponível em: https://www.mpmg.mp.br/data/files/80/10/52/54/DA44A7109CEB34A7760849A8/Tutela%20Inibitoria%20e%20Tutela%20de%20Remocao%20do%20Ilicito.pdf

proibindo a divulgação de um *deepfake* antes que este cause prejuízos maiores à vítima, amparando-se apenas no fato de tal conteúdo violar seu direito de imagem.

No contexto do MCI, a tutela inibitória se materializa via ordens judiciais de remoção de conteúdo. O art. 19 do MCI estabelece a necessidade de uma ordem judicial específica para responsabilizar provedores por conteúdo de terceiros – o que na prática exige que a vítima obtenha uma decisão judicial mandando retirar o conteúdo ilícito. Cumprida a ordem, o provedor evita responsabilidade; descumprida, incorre em responsabilidade civil subsidiária. Ou seja, o regime do MCI reforça a ideia de que a vítima deve recorrer ao Judiciário para fazer cessar violações online (salvo exceções legais), utilizando-se exatamente da tutela preventiva/inibitória disponível. Exemplo: no caso de um *deepfake* difamatório circulando em redes sociais, o lesado pode ingressar com ação pedindo inativação do vídeo – e o juiz, com base no art. 19 do MCI e art. 497 do CPC, pode conceder liminar determinando que a plataforma remova o conteúdo ofensivo.

Cumpre notar que o STF, em junho de 2025, ao julgar os RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533), relatoria dos ministros Dias Toffoli e Luiz Fux, respectivamente, declarou parcialmente inconstitucional o art. 19 do MCI, permitindo maior responsabilização de plataformas em certos casos de conteúdos ilícitos, indicando tendência de flexibilização da "reserva de jurisdição", sobretudo quando se trate de graves violações a direitos de personalidade (conforme disposto também no art. 21 do MCI para cenas de nudez).

O art. 21 do MCI, aliás, é fundamental no tema de remoção: ele excepciona a necessidade de ordem judicial nos casos de imagens de nudez ou sexo divulgadas sem consentimento – determinando que, havendo notificação do ofendido, o provedor deve remover prontamente tais conteúdos, sob pena de responder solidariamente. Essa disposição, aplicada a casos de "pornografia de vingança" ou *deepfake* pornográfico, confere uma tutela preventiva extrajudicial: a própria vítima pode notificar a plataforma para que o material íntimo seja tirado do ar. É um mecanismo ágil de remoção de conteúdo nocivo, alinhado à proteção da imagem e da privacidade sexual.

Assim, no âmbito dos *deepfakes*, se envolverem contexto sexual da pessoa (montagens pornográficas), a vítima tem direito a exigir a remoção imediata junto ao

provedor, independentemente de processo judicial, utilizando-se dessa ferramenta do MCI.

Em síntese, o ordenamento brasileiro articula múltiplos instrumentos preventivos: o direito material (art. 12 CC) assegura a possibilidade de cessar violações a personalidade; o processo civil (art. 497) fornece a tutela inibitória procedimental; e o Marco Civil cria o dever (após ordem judicial, ou de pronto nos casos de nudez) de retirada de conteúdos ilícitos. Esses mecanismos combinados permitem reagir com rapidez frente aos riscos trazidos pelos deepfakes, evitando que o dano se espalhe e ampliando a proteção efetiva dos direitos de personalidade na era digital.

4.3 Interpretação do art. 20 do CC para abranger imagens artificiais: "imagem algorítmica" e "imagem provável"

O art. 20 do CC dispõe que a divulgação não autorizada da imagem de uma pessoa pode ser proibida judicialmente, salvo situações de interesse público ou quando necessária à administração da justiça. Tradicionalmente, esse dispositivo referia-se à imagem fotográfica ou videográfica real da pessoa. Contudo, a doutrina moderna tem ampliado a interpretação para abarcar também as imagens artificiais geradas por algoritmos – entendidas como prolongamento da identidade visual do indivíduo. Assim, deepfakes, avatares digitais hiper-realistas ou até projeções de aparência futura ("imagens prováveis") devem ser considerados imagens tuteladas pelo art. 20, pois reproduzem traços identificadores da pessoa e podem lesar sua personalidade da mesma forma que uma fotografia comum.

Alguns juristas propõem até nomenclaturas específicas para essas categorias inovadoras. Fala-se em "imagem algorítmica" para designar a representação visual de alguém produzida por IA, distinguindo-a da imagem tradicional (fotográfica). Também utiliza-se o termo "imagem provável" para situações em que sistemas preditivos geram uma figura de determinada pessoa (por exemplo, envelhecimentos simulados ou reconstruções faciais) – ou seja, uma imagem que a pessoa não chegou a encenar na vida real, mas que o algoritmo cria como se fosse. A justificativa para abranger essas variantes no conceito legal de imagem é clara: o bem jurídico protegido (a identidade visual e a honra associada a ela) permanece o mesmo. Pouco importa se a figura foi captada por uma câmera ou sintetizada por computador – se aquele conteúdo visual remete de forma

reconhecível a certa pessoa, está presente o direito à imagem e incide a tutela do art. 20 do CC.

Doutrinadores como Bruno Sartori Borges Júnior (2020) argumentam que a personalidade digital requer esse alargamento conceitual. Ele cunha a expressão "imagem algorítmica" exatamente para enfatizar que não se trata de uma fotografia, mas de uma criação algorítmica da aparência alheia. Tal conceito englobaria, por exemplo, vídeos *deepfake* em que o rosto de um ator é substituído pelo de outra pessoa: embora nenhum fotograma real dessa pessoa tenha existido, o resultado visual simula sua imagem pública – devendo ser protegido. Já a ideia de "imagem provável" aparece em propostas doutrinárias no contexto de tecnologias preditivas (como softwares de face swap ou aging): seriam aquelas imagens geradas a partir de dados da pessoa (fotos anteriores, padrões biométricos) para ilustrar uma aparência hipotética (como "assim Fulano ficaria mais velho" ou "assim seria Fulano se tivesse certas características"). Essas representações prováveis não deixam de ser extensões da imagem da pessoa, motivo pelo qual alguns autores sugerem incluí-las na guarida do art. 20. Afinal, se utilizadas sem consentimento e de modo ofensivo, podem violar tanto quanto uma foto verdadeira.

Embora não haja, ainda, legislação expressa no Brasil definindo "imagem algorítmica" ou semelhante, já se observam esforços hermenêuticos e propostas legislativas para acompanhar o avanço tecnológico. A Comissão de Juristas do Senado que elaborou o anteprojeto de atualização do CC em 2024 discutiu normatizar a utilização de IA na imagem de pessoas falecidas, exigindo consentimento prévio em vida. O ministro Luis Felipe Salomão, que presidiu a comissão, exemplificou o caso do comercial em que a cantora Elis Regina, já falecida, "contracenou" com a filha via IA – ressaltando que isso não pode ficar só a critério dos herdeiros; a pessoa deve ter manifestado vontade em vida para autorizar. [35] Ou seja, já se reconhece que a projeção digital póstuma da imagem de alguém é uma utilização abrangida pelo direito de imagem, demandando autorização específica (novamente uma ampliação teleológica do art. 20).

Além disso, projetos doutrinários sugerem conceitos inovadores. Propõe-se definir em lei a "imagem sintética" ou "imagem não original" de uma pessoa como qualquer representação visual gerada por meios tecnológicos que reproduza sua

[35] CNN BRASIL. Usar imagem por IA pós-morte deve ser autorizada em vida, diz Salomão à CNN. 24 mai. 2025. Disponível em: https://www.cnnbrasil.com.br/politica/usar-imagem-por-ia-pos-morte-deve-ser-autorizada-em-vida-diz-salomao-a-cnn/

fisionomia ou performance. Essa definição teria o propósito de evitar lacunas: se o art. 20 for lido de forma estrita (apenas "retrato" ou "imagem" no sentido literal), alguns poderiam alegar que deepfakes não estariam cobertos. Para afastar essa brecha, a doutrina preconiza leitura aberta: onde a lei diz imagem, leia-se também avatar, holograma, representação digital ou qualquer forma de aparência identificável da pessoa. Essa linha interpretativa já encontra respaldo em decisões judiciais embrionárias. Por exemplo, em julhados sobre "fake videos" de celebridades, tribunais brasileiros têm concedido a mesma proteção que dariam a uma foto vazada – equiparando o *deepfake* à imagem comum para fins de tutela inibitória e indenização por dano moral.

Em conclusão, a tendência doutrinária é adequar o art. 20 do CC aos novos tempos, para que deepfakes e derivados não escapem do manto protetivo do direito à imagem. Conceitos como "imagem algorítmica" e "imagem provável" enriquecem o vocabulário jurídico e deixam claro que a persona digital de um indivíduo – por mais artificial que seja sua construção – pertence a ele e somente a ele. Assim, se terceiros se apropriam dessa identidade visual construída por IA sem permissão, estará configurado o uso indevido de imagem, com todas as consequências legais (cessação do uso, indenizações etc.) tal como prevê o art. 20 do CC e a jurisprudência consolidada sobre direito de imagem.

4.4 Proteção da imagem e dos dados biométricos: sinergia entre CC, LGPD, MCI e CDC

A tutela da imagem pessoal hoje não se restringe ao direito civil clássico – envolve um diálogo multinormativo com a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet (MCI) e até o Código de Defesa do Consumidor (CDC) – integração necessária uma vez que a imagem de uma pessoa frequentemente se conecta a dados pessoais e contexto de consumo digital, e essa articulação permite que maior proteção do indivíduo frente a novas tecnologias.

Bruno Bioni enfatiza, por exemplo, que uma fotografia ou vídeo em que alguém seja identificável constitui dado pessoal – mais ainda, dado biométrico sensível quando

utilizado para reconhecimento facial – nos termos da LGPD.[36] Assim, qualquer uso de imagem deve respeitar não só o direito de personalidade do art. 20 do CC, mas também as bases legais e princípios da LGPD (consentimento, finalidade, necessidade, etc.). Bioni alerta que capturar imagens de pessoas sem autorização e jogar sobre elas o ônus de pedir remoção viola a LGPD, que considera a imagem um dado pessoal sujeito à proteção.

Ou seja, a LGPD reforça o direito à imagem: além do art. 20 CC que exige consentimento para uso da imagem, a LGPD (art. 7º e art. 11, no caso de dados sensíveis) também exige base legal para tratar dados pessoais, especialmente biométricos. Logo, um *deepfake* que utilize o rosto de alguém sem aval infringe simultaneamente o CC e a LGPD. Em outras palavras, o direito civil (tutela da personalidade) e o direito de proteção de dados convergem para um objetivo: garantir que atributos pessoais (como a imagem) não sejam explorados abusivamente na economia digital.

Não por acaso, Flávio Tartuce afirma ser necessária "*um diálogo muito intenso entre a LGPD e o capítulo de direitos da personalidade do CC/02, bem como com a matéria de responsabilidade civil*". [37] Essa integração normativa permite suprir lacunas: o CC assegura meios de cessar e indenizar; a LGPD traz princípios específicos (como minimização, transparência) e a possibilidade de sanções administrativas; o CDC, por sua vez, ao tratar da oferta e publicidade, protege contra práticas enganosas envolvendo consumidores (p.ex., uso da imagem do consumidor em propaganda sem consentimento, ou *deepfake* induzindo consumidores a erro). De fato, o CDC se aplica quando há relação de consumo – e a imagem/dados biométricos podem entrar nessa seara.

Imagine-se uma aplicação de filtro de beleza por IA em um app de varejo: se esse tratamento for abusivo ou inseguro, o CDC fornece base para alegar defeito no serviço ou prática comercial abusiva, com responsabilidade objetiva do fornecedor por eventuais danos. [38] O CDC prevê responsabilidade objetiva por defeitos na informação fornecida

[36] BIONI, Bruno. Fotógrafos vendem fotos de atletas na rua sem consentimento: direito autoral ou um problema de proteção de dados? Blog Bruno Bioni, 12 mar. 2025. Disponível em: https://brunobioni.com.br/blog/namidia/fotografos-vendem-fotos-de-atletas-na-rua-sem-consentimento-direito-autoral-ou-um-problema-de-protecao-de-dados/ e BIONI, Bruno. *Direitos de imagem, fotografia em locais públicos e LGPD*. Blog GEN Jurídico, 01 out. 2025. Disponível em: https://blog.grupogen.com.br/juridico/postagens/artigos/fotografia-locais-publicos-lgpd-direitos-imagem/

[37] MIGALHAS. "Desafio", diz Tartuce sobre adaptação do Direito Civil às tecnologias. Migalhas, 19 out. 2022. Disponível em: https://www.migalhas.com.br/quentes/375604/desafio--diz-tartuce-sobre-adaptacao-do-direito-civil-as-tecnologias

[38] REIS, Francisca Sílvia da Silva. Deepfakes e práticas de consumo: integridade informacional, proteção de dados e direitos de personalidade na ordem econômica digital. Revista FT (Sistemas de Informação, v.

ao consumidor e um *deepfake* ou conteúdo manipulado pode ser visto como informação defeituosa se induzir o consumidor em erro. Assim, LGPD, CC e CDC formam uma tríade de proteção: sendo violada a imagem/dado, aciona-se tanto a esfera civil clássica quanto a de dados e consumo.

Bruno Bioni ressalta que a imagem facial se enquadra como dado pessoal sensível nos termos da LGPD, exigindo cuidados redobrados quanto à sua coleta, armazenamento, tratamento e eventual descarte. Em sua análise crítica sobre práticas cotidianas de captação de imagem, o autor destaca que mesmo registros realizados em locais públicos não estão isentos de proteção legal quando identificam claramente uma pessoa, sendo imprescindível a adoção de políticas claras de consentimento, segurança e eliminação de dados. A ausência desses cuidados, segundo ele, caracteriza não apenas infração à LGPD, mas também afronta ao direito de personalidade previsto na parte geral do Código Civil, evidenciando a necessidade de uma interpretação sistemática e harmônica entre os regimes legais aplicáveis.[39]

Bioni observa ainda, ao refletir sobre o tratamento da imagem à luz da LGPD, que a face humana, mesmo quando captada em locais públicos, se insere na categoria de dado pessoal sensível, exigindo tratamento jurídico cauteloso, com base nos princípios de necessidade, finalidade e segurança. Ele destaca que a "*ausência de uma política clara para o armazenamento e descarte das imagens evidencia o descumprimento das normas que exigem uma gestão responsável dos dados pessoais*. Ou seja, a captação ou o uso da imagem sem consentimento prévio, sobretudo quando comercializada ou tratada de forma automatizada, representa afronta à autodeterminação informacional do titular e exige um reequilíbrio entre liberdade econômica, direitos autorais e privacidade na sociedade digital.

Vale ressaltar que a LGPD traz critérios objetivos de responsabilização que dialogam com a teoria civilista do risco do empreendimento. Por exemplo, no caso de um aplicativo de fotos que exponha indevidamente os rostos de usuários, poder-se-á invocar a responsabilidade objetiva do fornecedor prevista no CDC e, simultaneamente, a

29, ed. 150/SET 2025). Disponível em: https://revistaft.com.br/deepfakes-e-praticas-de-consumo-integridade-informacional-protecao-de-dados-e-direitos-de-personalidade-na-ordem-economica-digital/

[39] BIONI, Bruno. Fotógrafos vendem fotos de atletas na rua sem consentimento: direito autoral ou um problema de proteção de dados? Blog Bruno Bioni, 12 mar. 2025. Disponível em: https://brunobioni.com.br/blog/namidia/fotografos-vendem-fotos-de-atletas-na-rua-sem-consentimento-direito-autoral-ou-um-problema-de-protecao-de-dados/

responsabilidade do controlador prevista na LGPD (art. 42), ambas sem necessidade de culpa, dada a natureza da atividade de risco. O CDC e a LGPD partilham do propósito de proteger a parte vulnerável: o consumidor e o titular dos dados, respectivamente. Logo, num evento danoso envolvendo imagem/dados, pode-se manejar argumentos de consumo e de dados pessoais conjuntamente, fortalecendo a posição da vítima.

Em resumo, a proteção da imagem e dos dados biométricos no Brasil é multifacetada. O Direito Civil fornece o fundamento básico da personalidade e a reparação por danos; a LGPD agrega princípios e sanções específicos para uso indevido de dados/imagens, tratando-as como questão de privacidade e controle informacional; o MCI lida com a responsabilização e remoção de conteúdo nas redes, instrumentalizando a tutela; e o CDC pode ser invocado quando a imagem/dado é explorado em relações de consumo.

4.4. Modelos normativos internacionais: AI Act (UE), legislações estaduais nos EUA e abordagem do Reino Unido

A resposta regulatória aos desafios da IA – incluindo *deepfakes* – tem seguido caminhos diversos no direito comparado, dos quais convém extrair lições e tendências. A União Europeia destaca-se por uma abordagem abrangente e preventiva com seu Ato de Inteligência Artificial (*Artificial Intelligence Act – "AI Act"*), enquanto os Estados Unidos adotam medidas fragmentadas sobretudo em nível estadual, e o Reino Unido opta por uma via flexível e principiológica. A análise comparativa desses modelos evidencia diferentes pesos entre inovação e proteção, oferecendo subsídios para o debate brasileiro.

Em primeiro lugar, o o *AI Act* classifica sistemas de IA por nível de risco e impõe obrigações proporcionais – da proibição de usos considerados de risco inaceitável (e.g., manipulação subliminar, vigilância social) até requisitos de transparência e segurança para IAs de risco limitado.[40] *Deepfakes*, em particular, receberam atenção: o *AI Act* exigirá que conteúdos gerados por IA que possam ser confundidos com reais sejam claramente rotulados como sintéticos. Em outras palavras, haverá obrigatoriedade de marcação – por exemplo, um vídeo deepfake deverá conter aviso visível de que é obra

[40] EUROPEAN COMMISSION. *Regulatory framework on artificial intelligence (AI Act)*. Bruxelas: European Commission, [s.d.]. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

artificial. Essa medida de transparência visa preservar a confiança informacional e combater fraudes e desinformação.

O *AI Act* também prevê mecanismos de rastreabilidade (traceability) para certos sistemas: fornecedores de IAGs terão de assegurar registro de seu processo e documentação técnica auditável, de forma que autoridades e terceiros possam verificar como o conteúdo foi produzido.

Ademais, no arcabouço europeu já vigente, o GDPR (Regulamento Geral de Proteção de Dados) fornece proteção a dados pessoais utilizados em deepfakes, e a Diretiva de Serviços Digitais de 2022 impõe responsabilidades às plataformas quanto a remoção de conteúdos ilícitos.

Em síntese, a UE caminha para um modelo preventivo e *ex ante*: impor obrigações de transparência (rotulagem de IA, aviso de interação com *chatbots*, etc.) e de qualidade/diligência (teste de viés, robustez) antes mesmo que o dano ocorra. A filosofia subjacente é criar um ambiente de IA confiável, mitigando riscos sem sufocar a inovação. No tocante a deepfakes, a UE já inseriu na legislação específica a preocupação com identificação obrigatória desses conteúdos, tornando-se referência global nessa seara.

Nos Estados Unidos, por outro lado, vigora um robusto arcabouço de liberdade de expressão, a chamada Primeira Emenda (*First Amendment*) que torna difícil regular conteúdos digitais sem esbarrar em debates constitucionais. Assim, a resposta regulatória tem vindo dos Estados e de leis pontuais, como por exemplo Califórnia e Texas, que proibiram o uso de *deepfakes* em campanhas eleitorais nos períodos próximos à votação, criminalizando a divulgação maliciosa de mídia sintética envolvendo candidatos sem aviso de falsidade.[41]

A Califórnia também tipificou o chamado "*deepfake pornography*", dando às vítimas direito de processar e obter danos estatutários elevados (recentemente, ampliou as penas, permitindo indenização de até US$ 250.000,00 por infração para quem criar ou divulgar pornografia *deepfake* sem consentimento)[42].

[41] CNN BRASIL. Eleições nos EUA: uso de deepfake e IA revela problema que pode se repetir no Brasil. CNN Brasil, 23 jan. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/eleicoes-nos-eua-uso-de-deepfake-e-ia-revela-problema-que-pode-se-repetir-no-brasil/

[42] SWISSINFO. Califórnia promulga 1ª lei nos EUA que exige medidas de segurança para chatbots de IA. 13 out. 2025. Disponível em: https://www.swissinfo.ch/por/calif%C3%B3rnia-promulga-1%C2%AA-lei-nos-eua-que-exige-medidas-de-seguran%C3%A7a-para-chatbots-de-ia/90161475

Conforme levantamento da Bloomberg, até início de 2024 apenas cinco estados (Califórnia, Texas, Michigan, Washington e Minnesota) tinham aprovado leis proibindo certos usos de IA em propaganda eleitoral, com outros sete estados em vias de aprovar, enquanto mais da metade permanecia sem regulação específica.[43]

Em resumo, o modelo americano é menos centralizado: privilegia remédios ex post (processos por difamação, invasão de privacidade) e regulações de nicho (lei eleitoral estadual, lei de direitos de imagem post-mortem em alguns estados como Nova York). A ausência de harmonização pode gerar insegurança jurídica e dificuldades de enforcement quando deepfakes circulam nacionalmente. Por outro lado, a forte tutela da liberdade de expressão lá impõe balizas: regulações precisam ser cirúrgicas para atingir apenas usos dolosos e não inviabilizar usos paródicos ou políticos legítimos.

O Reino Unido optou por não criar, até o momento, uma lei específica e rígida para IA. Em março de 2023, o governo britânico publicou um White Paper estabelecendo uma abordagem "pro-innovation" para a regulação de IA, ou seja, uma estratégia regulatória flexível, orientada por princípios e setorial.[44]

Em vez de um *AI Act* como o europeu, o Reino Unido propõe delegar a regulação da IA aos reguladores existentes (de setores como saúde, transporte, financeiro etc.), guiados por cinco princípios gerais: segurança, transparência, justiça, responsabilidade e contestabilidade. Essa abordagem descentralizada visa evitar excesso de regras que possam frear a inovação, apostando em guidelines não-vinculantes e boa governança corporativa.

Assim, não há imposição legal de rotulagem de *deepfakes* até agora, embora as grandes plataformas tenham se engajado em autorregulação, enfatizando soluções voluntárias e códigos de conduta, acreditando que um marco jurídico muito rígido poderia prejudicar o desenvolvimento da IA no país.

Ao fim, essa comparação internacional revela tendências complementares: a transparência emerge como denominador comum – seja via rotulagem obrigatória ou

[43] CNN BRASIL. Eleições nos EUA: uso de deepfake e IA revela problema que pode se repetir no Brasil. CNN Brasil, 23 jan. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/eleicoes-nos-eua-uso-de-deepfake-e-ia-revela-problema-que-pode-se-repetir-no-brasil/

[44] HUNTON ANDREWS KURTH LLP. UK Government publishes AI White Paper – A pro-innovation approach to AI regulation. Privacy & Information Security Law Blog, 29 mar. 2023. Disponível em: https://www.hunton.com/privacy-and-information-security-law/uk-government-publishes-ai-white-paper

recomendada – reconhecendo que informar o usuário quando um conteúdo é gerado por IA é crucial para combater fraudes. Outro ponto é a rastreabilidade e auditoria, fortemente destacadas na UE e debatidas globalmente, para permitir imputar responsabilidade e melhorar a segurança dos sistemas. Há ainda diferenças culturais: enquanto a UE privilegia o princípio da precaução (regras preventivas rígidas), os EUA escoram-se no controle pós-fato (litígio judicial, responsabilização após o dano) e o UK tenta equilibrar ambos via regulação leve e responsiva. Essas experiências fornecem um leque de opções que o Brasil pode observar ao moldar sua própria regulação de IA, conforme abordaremos a seguir.

4.5. Propostas normativas para regulação da IA no Brasil (marcação obrigatória, rastreabilidade, responsabilidade objetiva etc.)

No Brasil, o debate regulatório sobre IA ganhou força a partir de 2023, com diversas propostas legislativas e recomendações de especialistas focando em medidas concretas para mitigar os riscos de sistemas de IA, incluindo os deepfakes. Dentre as ideias em discussão destacam-se: a marcação obrigatória de conteúdo gerado por IA, a rastreabilidade dos processos algorítmicos, a adoção de um regime de responsabilidade civil objetiva para certos fornecedores de IA, além de requisitos de transparência, criação de autoridades supervisoras e outros mecanismos. Tais propostas refletem um esforço de alinhamento com tendências internacionais (como as do *AI Act*) e também uma resposta às especificidades do nosso ordenamento (por exemplo, aproveitar as bases da responsabilidade objetiva já existentes no CDC).

Uma medida muito salientada é a obrigatoriedade de rotulagem (watermarking) de conteúdos sintéticos. A ideia é estabelecer em lei que deepfakes ou mídias geradas por IA devam conter identificação visível informando seu caráter artificial. Essa marcação poderia ser um selo digital inserido no arquivo ou uma legenda indicativa na divulgação. A justificativa é reduzir o engano e facilitar a checagem de autenticidade. Projetos como o substitutivo da Câmara dos Deputados ao PL 21/2020 (Marco Legal da IA) já incluíam dispositivos impondo que o usuário seja alertado ao interagir com um sistema de IA (ex: um *chatbot*) e que conteúdos automatizados destinados a ampla difusão sejam sinalizados. Na comunidade técnica e jurídica, discute-se implementar marcas d'água

digitais e metadados verificáveis embutidos nos arquivos produzidos por IA.[45] Bioni, por exemplo, sugere a possibilidade de criar um "selo de origem" para vídeos, que permitiria identificar se um vídeo saiu diretamente de uma câmera ou se foi gerado por rede neural, bem como logs auditáveis e certificações independentes, que fossem incorporados ao ordenamento como presunções legais de veracidade ou falsidade. Isso auxiliaria vítimas de *deepfake* a provar a falsidade do conteúdo em juízo, invertendo o ônus da prova para o manipulador quando não houver selo.

Uma inspiração vem da China, que já em 2019 emitiu regulamentação exigindo rotulagem obrigatória de conteúdos "sintéticos", punindo severamente quem divulgar mídias alteradas sem aviso. Essa regra chinesa, apesar de inserida num contexto autoritário, demonstra eficácia em coibir deepfakes indetectáveis no cotidiano digital chinês.[46] No Brasil, a marcação obrigatória de deepfakes é vista com bons olhos por muitos especialistas, mas traz desafios: como garantir que atores maliciosos realmente apliquem o selo? Cogita-se a necessidade de envolvimento das plataformas: por exemplo, que redes sociais detectem e sinalizem conteúdo sintético não marcado. Em qualquer caso, a transparência obrigatória figura entre as principais propostas, por fortalecer a integridade informacional no ambiente digital.

Outra proposta recorrente é a da rastreabilidade e do dever de registro nos sistemas de IA. Isso significa exigir que desenvolvedores e operadores de IA mantenham logs e documentação sobre o funcionamento e decisões dos algoritmos – de modo similar ao previsto no AI Act europeu. No contexto de *deepfakes*, a rastreabilidade implicaria, por exemplo, conservar os registros de treino e os parâmetros utilizados para gerar determinada mídia sintética. Assim, se um vídeo falso calunioso surgisse, seria tecnicamente viável rastrear qual ferramenta o criou, que usuário a acionou, quais dados de fonte foram empregados etc., facilitando tanto a responsabilização do agente malicioso quanto a retirada coordenada do conteúdo em múltiplos locais.

Em relação à responsabilidade civil, discute-se se o regime tradicional (subjetivo, baseado em culpa) é adequado frente à complexidade e difusão das IAs. Muitos defendem

[45] REIS, Francisca Sílvia da Silva. Deepfakes e práticas de consumo: integridade informacional, proteção de dados e direitos de personalidade na ordem econômica digital. Revista FT (Sistemas de Informação, v. 29, ed. 150/SET 2025). Disponível em: https://revistaft.com.br/deepfakes-e-praticas-de-consumo-integridade-informacional-protecao-de-dados-e-direitos-de-personalidade-na-ordem-economica-digital/

[46] ZUBOFF, Shoshana. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.

adotar, para certos provedores de IA, um regime de responsabilidade objetiva – similar ao do CDC para produtos e serviços – o que significaria que se uma IA causar dano a alguém, o lesado não precisaria provar culpa ou dolo do desenvolvedor; bastaria demonstrar o nexo entre a IA e o dano.

Esse regime reconhece que IAs são atividades de risco, de modo que quem as coloca em funcionamento deve arcar com os prejuízos decorrentes, independentemente de falha específica. É justo que a IA seja tratada como "produto de risco", atraindo responsabilidade independentemente de culpa, cabendo ao fornecedor depois buscar direito de regresso se couber, uma vez que, conforme Hildebrandt: "*os deepfakes desafiam critérios de autenticidade probatória. A facilidade de adulteração digital torna necessária a adoção de presunções e de mecanismos de certificação técnica. Sem tais recursos, litígios envolvendo conteúdos manipulados podem se tornar insolúveis ou excessivamente custosos*".[47]

Nesse diapasão, a proposta seria: provedores de sistemas de IA de alto impacto respondem objetivamente por danos que suas aplicações causarem aos usuários ou terceiros, salvo se comprovarem que tomaram todas as medidas exigidas (uma espécie de inversão do ônus da prova de diligência). Essa calibragem de responsabilidades é delicada – há preocupação de não inibir startups ou inovação – por isso, algumas propostas preveem objetividade apenas para grandes operadores ou para usos específicos (ex: IA em saúde, transporte). Ainda assim, o consenso emergente é de ampliar a tutela das vítimas, seja via objetivação, seja via presunções de culpa ou deveres legais de segurança (que, se descumpridos, já caracterizam culpa do agente).

Outras ideias complementares incluem: (i) obrigação de avaliação de impacto de IA, exigindo que empresas façam relatórios de risco antes de lançar IA; (ii) criação de órgão regulador setorial, isso é, agência ou autarquia voltada para fiscalizar IA, ou fortalecer a ANPD para abarcar IA; (iii) incentivo à autorregulação responsável; e (iv) educação midiática da população por meio de políticas públicas para conscientizar usuários sobre *deepfakes*, reduzindo suscetibilidade à manipulação.

Em suma, o Brasil deve se inspirar nas experiências externas e em sua própria tradição jurídica para moldar uma regulação de IA híbrida: aproveitar o arcabouço

[47] HILDEBRANDT, Mireille. Smart technologies and the end(s) of law: novel entanglements of law and technology. Cheltenham: Edward Elgar, 2015.

existente (CC, CDC, LGPD, MCI), porém agregando regras novas que enfrentem peculiaridades tecnológicas (rotulagem, auditabilidade, responsabilidade por algoritmos opacos). As propostas de marcação obrigatória, rastreabilidade e responsabilidade objetiva figuram entre as mais consensuais para compor um futuro Marco Legal da IA.

Caso implementadas, elas colocarão o Brasil em sintonia com a vanguarda internacional e, ao mesmo tempo, reforçarão mecanismos domésticos de proteção do cidadão contra abusos digitais. O objetivo último é garantir transparência e segurança no uso da IA, de modo a colher seus benefícios inovadores sem sacrificar direitos fundamentais – uma preocupação que permeia todo o Capítulo 4 deste estudo.

CONCLUSÃO

A análise desenvolvida ao longo deste trabalho permitiu demonstrar que a ascensão das tecnologias de IAG – especialmente deepfakes e avatares digitais – inaugura um cenário de tensões inéditas para o direito de imagem no ordenamento jurídico brasileiro. Partindo do reconhecimento de que a imagem integra o núcleo essencial dos direitos da personalidade, protegida de forma ampla pelo Código Civil, pela Constituição Federal e por normativas setoriais como a LGPD, foi possível evidenciar que a emergência de mecanismos capazes de replicar, manipular e sintetizar identidades humanas com elevado grau de verossimilhança desafia as categorias tradicionais de consentimento, dano, autoria e responsabilidade civil.

Demonstrou-se, igualmente, que a exploração da imagem por sistemas algorítmicos não ocorre em um vácuo tecnológico, mas dentro de um ecossistema marcado por assimetrias informacionais, opacidade nos processos de machine learning e crescente capacidade de automação de conteúdos. Tais características tornam a produção digital um produto de risco, exigindo do direito respostas que conciliem liberdade tecnológica, segurança jurídica e proteção da dignidade humana. Nesse sentido, a jurisprudência e a doutrina vêm dando sinais de adaptação, ainda que de forma fragmentada, ao reconhecer a necessidade de atualizar os parâmetros de imputação de responsabilidade, reforçar deveres de transparência e ampliar a tutela preventiva.

A investigação também revelou que os deepfakes, em particular, abalam noções clássicas de autenticidade e confiabilidade probatória, impondo ao sistema de justiça o

desafio de distinguir, com rigor técnico, manifestações verdadeiras de simulações capazes de induzir condutas, manipular opiniões e afetar direitos econômicos e extrapatrimoniais. A ausência de critérios padronizados de verificação e a dificuldade de rastrear a origem de conteúdos sintéticos tornam essa tarefa ainda mais complexa, razão pela qual alguns ordenamentos estrangeiros já avançam em exigências específicas de rotulagem e certificação, movimento que tende a influenciar futuros caminhos regulatórios no Brasil.

Apesar das dificuldades identificadas, o estudo conclui que o arcabouço jurídico brasileiro dispõe de fundamentos sólidos para tutelar o direito de imagem diante desses novos riscos. O sistema de responsabilidade civil, aliado à proteção constitucional da personalidade e às normas de proteção de dados, fornece instrumentos suficientes para coibir abusos, exigir reparação e limitar usos indevidos da identidade visual de indivíduos. Contudo, tais instrumentos somente alcançarão eficácia plena se acompanhados de evolução doutrinária, atualização legislativa pontual e interiorização, pelos agentes econômicos, de padrões mínimos de governança algorítmica.

Assim, mais do que propor rupturas, a conclusão que se impõe é a de que o direito positivo brasileiro já aponta caminhos para o enfrentamento dos desafios trazidos pela IAG, mas sua aplicação prática demanda interpretações sensíveis ao contexto tecnológico contemporâneo. A proteção da imagem – enquanto expressão da dignidade e projeção da identidade no espaço público digital – continuará sendo um dos eixos centrais desse processo de adaptação normativa. A consolidação de soluções estáveis exigirá, portanto, que o desenvolvimento tecnológico caminhe lado a lado com mecanismos jurídicos mais claros, procedimentos probatórios mais robustos e uma compreensão cada vez mais refinada das fronteiras entre criação, manipulação e representação digital.

Em última análise, o direito de imagem permanece como um campo vivo e em constante transformação, convocando juristas, legisladores, plataformas e sociedade civil a construir respostas articuladas, capazes de preservar a autonomia individual sem sufocar a inovação. Este trabalho buscou contribuir para essa reflexão, demonstrando que a tecnologia não supera o direito: ao contrário, provoca-o a evoluir, reafirmando a centralidade da pessoa humana no centro da ordem jurídica, mesmo – e sobretudo – em tempos de inteligência artificial.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

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 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.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 12 set. 1990.

BRASIL. Superior Tribunal de Justiça. Súmula 403: Independe de prova do prejuízo a indenização pela publicação não autorizada da imagem de pessoa com fins econômicos ou comerciais.

CNN BRASIL. Disputa entre Scarlett Johansson e OpenAI realça temor de Hollywood com IA. São Paulo, 21 maio 2024. Disponível em: https://www.cnnbrasil.com.br/entretenimento/disputa-entre-scarlett-johansson-e-openai-realca-temor-de-hollywood-com-ia/.

FORBES BRASIL. O que o caso Taylor Swift nos alerta sobre os perigos da IA. São Paulo, 18 jan. 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/01/o-que-o-caso-taylor-swift-nos-alerta-sobre-os-perigos-da-ia/.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo Curso de Direito Civil: parte geral. São Paulo: Saraiva, 2002, p.183

BITTAR, Carlos Alberto. Os direitos da personalidade. Rio de Janeiro, Forense, 2ª ed., 1995, p.87

DINIZ, Maria Helena. Código Civil Anotado. 12.ed., rev. e atual. São Paulo: saraiva, 2005.

DINIZ, Maria Helena, Direito à imagem e sua tutela, In: BITTAR Eduardo C. B.; ALMEIDA, Silmara J. A. Chinelato e (coords). Estudos de direito de autor, direito da personalidade, direito do consumidor e danos morais. Forense Universitária, 2002. p. 79 e 80

DINIZ, Maria Helena. Curso de direito civil brasileiro, volume 1: teoria geral do direito civil. 32. ed. São Paulo: Saraiva, 2015, p. 147.

RODRIGUES, Silvio. Direito Civil: parte geral. 34.ed., São Paulo: Saraiva, 2003, p.74

SILVÉRIO, Michele de Cassia Tesseroli. O contrato de licença de uso de imagem e o direito do trabalho. 2004. Monografia (Bacharelado em Direito) — Universidade Federal do Paraná, Setor de Ciências Jurídicas, Curitiba, 2004. Disponível em: https://acervodigital.ufpr.br/xmlui/bitstream/handle/1884/48206/M456.pdf?sequence=1&isAllowed=y#:~:text=%E2%80%9CO%20direito%20%C3%A0%20imagem%20possui,A%20imagem%2C%20assim%2C%20tem%20duas

BRESCIANI, Felipe Passos. Proteção do direito à imagem como dado pessoal e como direito da personalidade: um estudo comparativo. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) — Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2023. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/41017

TARTUCE, Flávio. *Manual de direito civil: volume único.* 7ª ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2017.

RODRIGUES, Natália Bernadeth Fernandes; ARAÚJO, Anne de Fátima Pedrosa. Direitos da personalidade. Jus.com.br, 09 jan. 2017. Disponível em: https://jus.com.br/artigos/55019/direitos-da-personalidade

MEDON, Filipe. *O direito à imagem na era das deepfakes*. Revista Brasileira de Direito Civil – RBDCivil, v.27, p. 251-277, jan./mar. 2021. Disponível em: rbdcivil.ibdcivil.org.br. Acesso em: 15 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Quarta Turma nega à atriz Deborah Secco pedido de danos morais contra Editora Abril*. Brasília: STJ, 28 out. 2014. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2014/2014-10-28_17-55_Quarta-Turma-nega-a-atriz-Deborah-Secco-pedido-de-danos-morais-contra-Editora-Abril.aspx. Acesso em: 15 out. 2025.

MIGALHAS. *Justiça Eleitoral suspende perfil do Instagram por uso de deepfake*. Migalhas, 27 maio 2024. Disponível em: https://www.migalhas.com.br/quentes/408157/justica-eleitoral-suspende-perfil-de-instagram-por-uso-de-deepfake. Acesso em: 15 out. 2025.

FOLHA DE S. PAULO. *Nudes feitos com IA geram novos riscos para mulheres e esbarram em falta de regulação*. Folha de S.Paulo, São Paulo, 11 nov. 2023. Disponível em: https://www1.folha.uol.com.br/cotidiano/2023/11/nudes-feitos-com-ia-geram-novos-riscos-para-mulheres-e-esbarram-em-falta-de-regulacao.shtml. Acesso em: 18 out. 2025.

MARINONI, Luiz Guilherme. Tutela inibitória e tutela de remoção do ilícito. 2004. Disponível em: https://www.mpmg.mp.br/data/files/80/10/52/54/DA44A7109CEB34A7760849A8/Tutela%20Inibitoria%20e%20Tutela%20de%20Remocao%20do%20Ilicito.pdf. Acesso em 9 nov. 2025.

DONEDA, Danilo; ALMEIDA, Virgílio; LEMOS, Ronaldo. *Com avanço tecnológico, fake news vão entrar em fase nova e preocupante*. Disponível em: https://doneda.net/com-avanco-tecnologico-fake-news-vao-entrar-em-fase-nova-e-preocupante/#:~:text=deep%20fake%20news,relat%C3%B3rio%20do%20Conselho%20da%20Europa. Acesso em: 9 nov. 2025.

JUSBRASIL. *Piadas, sátiras e o limite do humor: a proteção jurídica dos comediantes*. JusBrasil, 17 mar. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/piadas-saturas-e-o-limite-do-humor-a-protecao-juridica-dos-comediantes/3228223237. Acesso em: 26 out. 2025.

ARTIFICIAL INTELLIGENCE ACT. *AI Act: The European regulation on Artificial Intelligence*. [S.l.], 2024. Disponível em: https://artificialintelligenceact.eu/.

TEFFÉ, Chiara Spadaccini de. Considerações sobre a proteção do direito à imagem na internet. *Revista de Informação Legislativa*, Brasília, v. 54, n. 213, p. 173-198, jan./mar. 2017. Disponível em: https://www.senado.leg.br/ril.

ROSSETTI, Regina; GARCIA, Kethly. Inteligência artificial generativa: questões jurídicas e éticas em torno do ChatGPT. *VirtuaJus*, Belo Horizonte, v. 8, n. 15, p. 253-264, 2º sem. 2023. ISSN 1678-3425. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/30769 .

HILDEBRANDT, Mireille. Smart technologies and the end(s) of law: novel entanglements of law and technology. Cheltenham: Edward Elgar, 2015.