

Rotulagem de conteúdo sintético e dever jurídico de transparência: limites de licitude no uso comercial da inteligência artificial generativa

Labeling of synthetic content and the legal duty of transparency: limits of lawfulness in the commercial use of generative artificial intelligence

José Luiz de Moura Faleiros Júnior¹

Resumo: O artigo analisa a rotulagem de conteúdo sintético gerado ou manipulado por inteligência artificial generativa como dever jurídico de transparência e seus limites de licitude no uso comercial. A partir de perspectiva dogmático-jurídica, regulatória e consumerista, examina os fundamentos normativos do dever de identificar conteúdos artificialmente produzidos ou substancialmente modificados, incluindo *deepfakes*, avatares sintéticos, clones de voz e influenciadores virtuais, com ênfase nos direitos da personalidade, no dever de informação, na vedação à publicidade enganosa e na responsabilidade civil dos agentes econômicos. A hipótese central sustenta que a rotulagem constitui dever jurídico autônomo de transparência, extraível do sistema brasileiro de proteção da confiança, da boa-fé objetiva, da proteção de dados pessoais e da tutela do consumidor, mas possui função limitada: a identificação da natureza sintética do conteúdo não legitima, por si só, sua circulação quando houver uso não autorizado de imagem, voz ou identidade, tratamento irregular de dados pessoais, publicidade enganosa ou violação de direitos da personalidade. A rotulagem é condição de transparência, não condição suficiente de licitude. A metodologia é dogmático-dedutiva, com revisão bibliográfica especializada, análise normativa do direito brasileiro vigente e exame de parâmetros regulatórios comparados, especialmente o AI Act europeu e o Digital Services Act. Conclui-se que a licitude do conteúdo sintético exige arquitetura de transparência composta por rotulagem, consentimento, proteção de dados, tutela do consumidor, *accountability* e responsabilidade civil multissubjetiva.

Palavras-chave: conteúdo sintético. deepfake. transparência. direitos da personalidade. inteligência artificial generativa.

Abstract: This article analyzes the labeling of synthetic content generated or manipulated by generative artificial intelligence as a legal duty of transparency and its limits of lawfulness in commercial use. From a dogmatic-legal, regulatory, and consumer protection perspective, it

¹ Doutor em Direito Civil pela Universidade de São Paulo (USP) e Doutor em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais (UFMG). Mestre e Bacharel em Direito pela Universidade Federal de Uberlândia (UFU). Pós-doutor em Direito Privado pela Universidade Federal do Rio Grande do Sul (UFRGS). Professor da Faculdade Milton Campos (FMC) e da Skema Law School. Advogado. ORCID: <https://orcid.org/0000-0002-0192-2336>. E-mail: josefaleirosjr@outlook.com

examines the normative foundations of the obligation to identify artificially produced or substantially modified content — including deepfakes, synthetic avatars, voice clones, and virtual influencers —, with emphasis on personality rights, the duty of information, the prohibition of misleading advertising, and the civil liability of economic actors. The central hypothesis holds that labeling constitutes an autonomous legal duty of transparency, derivable from the Brazilian system of trust protection, objective good faith, personal data protection, and consumer law, but has limited function: the identification of the synthetic nature of the content does not, by itself, legitimize its circulation when there is unauthorized use of image, voice, or identity, unlawful processing of personal data, misleading advertising, or violation of personality rights. Labeling is a condition of transparency, not a sufficient condition of lawfulness. The methodology is dogmatic-deductive, supported by specialized bibliographic review, normative analysis of current Brazilian law, and examination of comparative regulatory parameters, especially the European AI Act and the Digital Services Act. It concludes that the lawfulness of synthetic content requires a transparency architecture composed of labeling, consent, data protection, consumer law, accountability, and multi-subject civil liability.

Keywords: synthetic content. deepfake. transparency. personality rights. generative artificial intelligence.

1. Introdução

A inteligência artificial generativa alterou as condições técnicas de produção, modificação e circulação de conteúdos digitais. Imagens, vídeos, vozes e textos que antes eram ordinariamente associados a registros humanos ou a eventos captados da realidade podem agora ser fabricados, recombinaados ou manipulados por sistemas capazes de simular rostos, timbres, gestos, ambientes, estilos e declarações com elevado grau de verossimilhança. Essa transformação não produz apenas um problema tecnológico de detecção de falsidades. Ela afeta categorias jurídicas estruturantes do direito privado, como autenticidade, confiança, consentimento, identidade, informação e imputação de responsabilidade.

O conteúdo sintético, para os fins deste artigo, não é juridicamente relevante apenas porque resulta de inteligência artificial. Sua relevância decorre da aptidão para produzir falsa autenticidade, isto é, para fazer circular uma representação artificial como se fosse manifestação, presença, endosso, experiência ou identidade de pessoa real. *Deepfakes*, clones de voz,

avatares hiper-realistas e influenciadores virtuais tornam particularmente sensível essa questão quando se inserem em contextos comerciais, publicitários ou de monetização digital. Nesses ambientes, a artificialidade não revelada, ou revelada de modo insuficiente, pode interferir na formação da confiança do consumidor, na exploração econômica da imagem e da voz, no tratamento de dados pessoais e na tutela dos direitos da personalidade.

A rotulagem de conteúdo sintético surge, nesse cenário, como uma das respostas regulatórias mais relevantes. Identificar que determinada imagem, vídeo, áudio ou comunicação foi gerado ou substancialmente manipulado por inteligência artificial permite recompor, ao menos parcialmente, a assimetria informacional entre quem produz, distribui ou monetiza o conteúdo e quem é por ele afetado. O *AI Act* europeu (Regulamento 2024/1689(EU)), especialmente em seu art. 50, e as discussões brasileiras em torno do Projeto de Lei n.º 2.338/2023 evidenciam a tendência de converter a identificação de conteúdos artificiais em obrigação jurídica específica. No direito brasileiro vigente, embora inexista ainda disciplina geral e autônoma sobre conteúdo sintético, o dever de rotulagem pode ser extraído de uma leitura sistemática do Código de Defesa do Consumidor, do Código Civil, da Lei Geral de Proteção de Dados Pessoais e do Marco Civil da Internet.

O ponto decisivo, contudo, está em evitar que a rotulagem seja convertida em salvo-conduto. A informação de que certo conteúdo foi produzido por IA pode ser juridicamente necessária, mas não torna automaticamente lícita a utilização de imagem, voz, nome, identidade pessoal, dados biométricos ou aparência de endosso de pessoa real. Tampouco impede a configuração de publicidade enganosa, publicidade velada, tratamento irregular de dados pessoais ou responsabilidade civil por danos individuais e coletivos. A transparência sobre a artificialidade do conteúdo é apenas uma das camadas de licitude, não substituindo o consentimento, a finalidade legítima, a não enganosidade e o respeito aos direitos da personalidade.

Diante disso, o problema de pesquisa que orienta o presente artigo é o seguinte: a rotulagem de conteúdo sintético produzido ou manipulado por inteligência artificial pode operar como mecanismo suficiente de transparência e legitimação jurídica, ou deve ser compreendida apenas como dever informacional mínimo, incapaz de suprir consentimento, licitude do tratamento de dados e respeito aos direitos da personalidade?

A hipótese central é a de que a rotulagem de conteúdo sintético constitui dever jurídico autônomo de transparência, extraível do sistema brasileiro de proteção da confiança, do dever de informação, da boa-fé objetiva, da proteção de dados pessoais e da tutela do consumidor. Todavia, esse dever possui função limitada: a identificação da natureza sintética do conteúdo não legitima, por si só, sua circulação quando houver uso não autorizado de imagem, voz ou identidade, tratamento irregular de dados pessoais, falsa impressão de endosso, publicidade enganosa ou violação de direitos da personalidade. A rotulagem, portanto, é condição de transparência, mas não condição suficiente de licitude.

A metodologia adotada é dogmático-dedutiva, com revisão bibliográfica especializada, análise normativa do direito brasileiro vigente e exame de parâmetros regulatórios comparados, especialmente o *AI Act* europeu e o *Digital Services Act*. O artigo desenvolve-se em três movimentos. Primeiro, delimita o conteúdo sintético como problema jurídico de autenticidade, confiança e consentimento. Em seguida, demonstra a rotulagem como dever jurídico de transparência fundado no direito privado brasileiro e reforçado por tendências regulatórias internacionais. Por fim, examina os limites da rotulagem nos campos da personalidade, da publicidade sintética e da responsabilidade civil das plataformas e demais agentes econômicos.

2. Conteúdo sintético, autenticidade e confiança

O conteúdo sintético, para os fins deste artigo, é todo conteúdo digital, imagens, vídeos, áudios, textos ou formatos multimodais, substancialmente gerado, modificado ou simulado por sistemas de inteligência artificial, com aptidão para produzir representações realistas de pessoas, eventos, objetos, ambientes ou declarações. Sua relevância jurídica não decorre da artificialidade em si, mas da capacidade de fazer circular representações artificiais como se fossem expressões autênticas de identidade, presença, endosso ou experiência de pessoa real. É essa aptidão para a falsa autenticidade que confere ao conteúdo sintético sua específica relevância para o direito privado.

O *deepfake* consiste em vídeo, imagem ou áudio no qual a aparência, a voz ou as declarações de uma pessoa real são fabricadas ou sobrepostas por redes neurais profundas, criando a impressão de que determinada pessoa disse ou fez algo que, na realidade, não ocorreu. O clone de voz reproduz sinteticamente o timbre, o ritmo, a entonação e a dicção de uma pessoa específica, gerando falas jamais proferidas. O avatar hiper-realista pode assemelhar-se intensamente a alguém real ou constituir entidade fictícia projetada para interagir com usuários como se fosse humana. O influenciador virtual insere-se em comunicações comerciais sem revelar, adequadamente, sua natureza artificial. É possível sintetizar os desafios dessas tecnologias ao analisar a recriação de artistas falecidos em campanhas publicitárias, evidenciando que os avanços tecnológicos tornaram possível recriar imagens e áudios de pessoas de forma extremamente realista, o que levanta sérias questões sobre privacidade, autenticidade e o uso não autorizado dessas representações (Silveira; Faleiros Júnior, 2024, p. B1). Essas categorias, analiticamente distinguíveis, frequentemente se combinam em práticas concretas de comunicação, publicidade e entretenimento, impondo ao direito o desafio de respostas que abranjam a categoria ampla, e não apenas cada manifestação isolada.

O crescimento exponencial dessas tecnologias já é documentado empiricamente. Ajder *et al.* (2019) mapearam o estado dos *deepfakes* em relatório que identificou sua disseminação majoritária em conteúdo sexualmente explícito não consentido, com aceleração significativa de usos políticos, fraudulentos e comerciais. Chesney e Citron (2019, p. 1753) identificaram os *deepfakes* como um desafio iminente para a privacidade, a democracia e a segurança nacional, demonstrando que a capacidade de fabricar representações convincentes de comportamentos humanos desestabiliza fundamentos epistêmicos de múltiplas instituições sociais. A inteligência artificial generativa ultrapassa os limites da automação tradicional, pois passa a produzir conteúdos dotados de aparente autonomia criativa, fenômeno que suscita implicações éticas e jurídicas de elevada complexidade, cujas respostas regulatórias ainda se encontram em processo de construção (Borges; Mello Filho, 2023, p. 284).

No plano jurídico, a crise da autenticidade produz consequências em quatro campos principais. No campo probatório, um vídeo ou áudio fabricado pode ser apresentado como falsa evidência em litígios, negociações ou campanhas de desinformação. No campo do consentimento, a manifestação aparentemente atribuída a uma pessoa pode ter sido sinteticamente produzida, comprometendo a atribuição de vontade e a formação de vínculos jurídicos. No campo reputacional, alguém pode ser submetido a fabricações danosas à honra, à imagem, à privacidade e à integridade psíquica. No campo da confiança comercial, consumidores podem ser induzidos a decisões de consumo com base em endossos, depoimentos ou apresentações artificiais. Essa desestabilização desafia a boa-fé objetiva, consagrada nos arts. 113, 187 e 422 do Código Civil, o dever de informação previsto no art. 6.º, III, do Código de Defesa do Consumidor, e a proteção constitucional dos direitos da personalidade, prevista no art. 5.º, V e X, da Constituição Federal de 1988.

É importante ressaltar, contudo, que nem todo conteúdo sintético é juridicamente ilícito. Paródias, sátiras, obras ficcionais, produções artísticas

e usos transparentemente contextualizados podem legitimamente empregar técnicas de IA, desde que observados os limites decorrentes dos direitos da personalidade, da boa-fé objetiva, do dever de informação e da vedação ao uso enganoso. A relevância jurídica do conteúdo sintético está em sua aptidão para produzir falsa autenticidade, não na artificialidade como tal. Essa distinção é essencial para evitar que a regulação da IA generativa se converta em proibição geral de um recurso tecnológico que também serve a usos lícitos, criativos e socialmente valiosos. A tensão entre liberdade de expressão, inovação tecnológica e proteção de direitos individuais é estrutural ao tema e exige critérios normativos de diferenciação, não supressão.

3. Rotulagem como dever jurídico de transparência

3.1. A rotulagem no sistema de deveres informacionais

A rotulagem de conteúdo sintético deve ser compreendida no interior do sistema jurídico dos deveres informacionais, especialmente a partir do princípio da boa-fé objetiva e do dever geral de transparência. Em seu sentido mais amplo, rotular significa identificar, de modo adequado e suficientemente perceptível, que determinado conteúdo foi gerado ou substancialmente modificado por inteligência artificial, permitindo que seus destinatários o avaliem a partir de uma percepção minimamente adequada de sua natureza e origem. No direito brasileiro vigente, o dever de rotulagem pode ser extraído de uma leitura sistemática de quatro pilares normativos: o Código de Defesa do Consumidor, o Código Civil, a Lei Geral de Proteção de Dados Pessoais e o Marco Civil da Internet.

O Código de Defesa do Consumidor oferece o fundamento mais direto. O art. 6.º, III, consagra como direito básico do consumidor a informação adequada e clara sobre os diferentes produtos e serviços. O art. 31 impõe que a oferta e a apresentação assegurem informações corretas, claras, precisas e ostensivas. Interpretados em conjunto com a vedação à publicidade enganosa

(art. 37, § 1.º) e à publicidade velada (art. 36, caput), esses dispositivos permitem afirmar que, em qualquer comunicação comercial, a natureza sintética do conteúdo deve ser identificada de modo claro e perceptível pelo consumidor médio. A linha entre publicidade sintética lícita e publicidade enganosa passa pela adequação do rótulo: informação discreta, periférica, técnica ou temporariamente breve não satisfaz o dever de informação ostensiva.

O Código Civil contribui por meio da cláusula geral de boa-fé objetiva, prevista no art. 422, que impõe às partes de qualquer relação jurídica deveres de lealdade, cooperação e informação. A boa-fé objetiva não se limita à vedação de condutas dolosas: ela impõe deveres anexos de conduta, entre os quais o dever de não omitir informações relevantes para a formação da vontade alheia. A omissão quanto à natureza artificial de um vídeo, imagem ou voz pode configurar violação ao dever de informação, com potencial de gerar responsabilidade civil nos termos do art. 186, inclusive nas relações extracontratuais.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) acrescenta camadas normativas relevantes sempre que o conteúdo sintético envolver dados biométricos, imagens faciais, padrões vocais ou quaisquer atributos identificáveis de pessoa natural. Esses dados qualificam-se como dados pessoais sensíveis (art. 5.º, II, da LGPD), sujeitos a regime jurídico reforçado que exige, na ausência de outra base legal adequada, consentimento específico e destacado (art. 11, I). Os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização (art. 6.º da LGPD) incidem sobre todo o ciclo de vida do conteúdo sintético que envolva dados pessoais, desde a coleta e o treinamento do modelo até a distribuição e monetização do produto final. A rotulagem é, nesse contexto, condição de transparência no sentido da LGPD, mas não esgota as exigências normativas da lei.

O Marco Civil da Internet, por sua vez, estabelece os parâmetros gerais de responsabilidade dos provedores de aplicações (art. 19), além de impor deveres de proteção de dados e privacidade (arts. 7.º e 8.º). Para fins de rotulagem, o Marco Civil é relevante especialmente para delimitar a posição das plataformas como intermediárias, hospedeiras ou distribuidoras de conteúdo produzido por terceiros. Em conjunto, esses quatro diplomas formam o substrato normativo a partir do qual se pode afirmar, no direito brasileiro vigente, a existência de um dever jurídico de rotulagem do conteúdo sintético, ainda que não haja disciplina geral e específica sobre o tema.

3.2. Parâmetros regulatórios internacionais e o PL 2.338/2023

No plano internacional, o Regulamento (UE) 2024/1689, conhecido como *AI Act*, estabelece, em seu art. 50, obrigações específicas de transparência para sistemas de IA que produzam ou manipulem conteúdo de imagem, áudio ou vídeo de modo a criar representações falsas da realidade, incluindo *deepfakes*. Nesses casos, os operadores de sistemas de IA devem assegurar que o conteúdo seja identificado como artificialmente gerado ou manipulado por meios técnicos adequados, e que essa identificação seja transmitida de modo interoperável, detectável por máquinas e processável de modo automatizado. A exceção cobre usos legitimamente autorizados no contexto do exercício da liberdade de expressão artística e criativa, quando acompanhados de divulgação adequada.

O *AI Act* adota uma lógica de proporcionalidade baseada em classificação por risco. Sistemas de IA de alto risco — em áreas como educação, emprego, saúde, infraestrutura crítica, segurança pública e administração da justiça — estão sujeitos a obrigações mais intensas de governança, auditoria, rastreabilidade e conformidade. Para os sistemas generativos de uso geral (GPAI), o regulamento impõe deveres adicionais de transparência e avaliações de risco sistêmico para os modelos mais

avancados. Essa lógica de proporcionalidade oferece um modelo regulatório que o direito brasileiro ainda não consolidou de modo específico para o conteúdo sintético.

O *Digital Services Act*, Regulamento (UE) 2022/2065, complementa esse quadro ao impor às plataformas online de grande porte deveres específicos de avaliação e mitigação de riscos sistêmicos relacionados à desinformação, incluindo conteúdos gerados ou manipulados por IA (arts. 34 e 35). A responsabilidade das plataformas não se esgota na hospedagem passiva: quando atuam ativamente na recomendação, amplificação ou monetização de conteúdo, devem adotar medidas proporcionais de mitigação de riscos.

No Brasil, o Projeto de Lei n.º 2.338/2023, em tramitação na Câmara dos Deputados, constitui a principal proposta de regulação específica de inteligência artificial. O projeto adota classificação de sistemas de IA por nível de risco e prevê deveres de transparência, informação, governança e responsabilização aplicáveis ao desenvolvimento e ao uso de sistemas de IA em território nacional. No que tange ao conteúdo sintético, o projeto inclui previsões sobre a necessidade de identificação da natureza artificial de comunicações e sobre os deveres das plataformas diante de conteúdos de alto risco. Embora ainda em tramitação e passível de alterações, o PL 2.338/2023 sinaliza a tendência do ordenamento brasileiro de converter a rotulagem em obrigação específica, alinhada às melhores práticas internacionais. A leitura sistemática entre o direito vigente e as propostas regulatórias em curso permite afirmar que o dever de rotulagem já possui fundamento normativo suficiente no direito brasileiro, ainda que careça de disciplina específica.

3.3. A arquitetura de transparência

A análise do quadro normativo revela que a rotulagem adequada de conteúdo sintético não pode ser reduzida a uma simples expressão textual,

como "feito por IA" ou "conteúdo gerado por inteligência artificial", inserida de modo perfunctório em legenda, rodapé ou metadado invisível ao usuário. A efetividade jurídica da rotulagem depende de sua arquitetura, isto é, do conjunto de mecanismos técnicos e comunicativos que, articulados, asseguram a perceptibilidade, a verificabilidade e a rastreabilidade da natureza sintética do conteúdo.

Uma arquitetura de transparência adequada compreende, no mínimo, três camadas funcionais. A primeira é a camada de sinalização perceptível ao usuário: advertência visível, clara e ostensiva, posicionada de modo que o consumidor médio a identifique de maneira imediata, sem esforço ou pesquisa adicional. Rótulos discretos, de baixo contraste, temporariamente breves, em idioma ou formato técnico inacessível ao destinatário médio, não satisfazem o dever de informação ostensiva previsto no art. 31 do CDC.

A segunda é a camada de credenciais de conteúdo e proveniência técnica: metadados estruturados, assinaturas digitais e registros de histórico de edição capazes de indicar origem, autoria e modificações do conteúdo de modo verificável por ferramentas independentes. A *Coalition for Content Provenance and Authenticity* (C2PA, 2026) desenvolveu especificação técnica aberta que permite incorporar ao arquivo digital um registro assinado de sua cadeia de produção, editores e modificações. O projeto *Content Credentials* (2026), baseado nessa especificação, oferece implementação acessível para criadores, plataformas e consumidores, com potencial para integração a sistemas de verificação automatizada. A terceira é a camada de governança e rastreabilidade sistêmica: procedimentos institucionais de controle, auditoria, notificação e resposta, que assegurem que a rotulagem seja aplicada de modo consistente, verificável e não fraudável ao longo do ciclo de vida do conteúdo.

É importante destacar, contudo, que mesmo essa arquitetura possui limitações técnicas significativas. A *National Security Agency* e agências parceiras (2025) alertam que credenciais de conteúdo podem ser removidas

quando o arquivo é publicado em plataformas que não as preservam, quando o conteúdo passa por conversões de formato, ou quando os metadados são deliberadamente eliminados. Marcas d'água imperceptíveis (*watermarks*) apresentam fragilidades similares. Por isso, a arquitetura de transparência deve ser compreendida como infraestrutura de governança e prova — não como mecanismo infalível de autenticação. A sua existência e integridade são relevantes para a aferição da boa-fé dos agentes, para a demonstração de conformidade normativa e para a instrução de processos judiciais e administrativos, mas não esgotam o juízo de licitude do conteúdo.

4. Os limites jurídicos da rotulagem

4.1. Imagem, voz, identidade e consentimento

O primeiro limite da rotulagem reside no campo dos direitos da personalidade: a identificação da natureza sintética do conteúdo não substitui o consentimento do titular dos atributos utilizados, nem afasta a incidência dos direitos da personalidade quando houver uso não autorizado de imagem, voz, nome ou identidade de pessoa real.

O art. 20 do Código Civil estabelece que a utilização da imagem de uma pessoa pode ser proibida pelo retratado, a requerimento do próprio ou de seus herdeiros, sempre que atingir a honra, a boa fama ou a respeitabilidade, ou se destinar a fins comerciais, ressalvadas as hipóteses de notoriedade pública, necessidade pública ou administração da justiça. O direito à imagem possui fundamento simultaneamente constitucional, nos termos do art. 5.º, V e X, da Constituição Federal, e civil, possuindo natureza personalíssima e intransferível, como assinalam Alves, Moura e Gomes (2022, p. 179). Esse regime de proteção não se restringe à imagem-retrato, isto é, a representação física direta da pessoa por fotografia, vídeo ou ilustração. Alcança também a imagem-atributo, compreendida como o conjunto de características pessoais, reputacionais e identitárias associadas à projeção social da pessoa.

Chiara de Teffé (2018, p. 2) esclarece que o direito à imagem protege principalmente interesses existenciais da pessoa, sendo compreendido como um direito da personalidade por se encontrar intrinsecamente ligado ao indivíduo enquanto ser, refletindo a expressão de sua existência. Uma simulação sintética que reproduza a aparência de alguém, ainda que não baseada em fotografia ou vídeo pré-existente, viola o direito à imagem quando captura e explora comercialmente o substrato identitário da pessoa representada. A artificialidade do processo de produção não neutraliza o desvalor jurídico da apropriação identitária.

A proteção vocal também integra esse campo. O clone de voz reproduz sinteticamente timbre, ritmo, entonação e padrão de fala de uma pessoa específica, com aptidão para gerar declarações jamais proferidas. O art. 20 do Código Civil aplica-se, por extensão analógica, à voz como atributo da personalidade, dado que cumpre função identitária equivalente à da imagem, servindo à individualização, ao reconhecimento e à projeção social da pessoa. O uso não autorizado de clone vocal para fins publicitários, políticos ou comerciais configura violação autônoma dos direitos da personalidade, independentemente de o produto final ser rotulado como sintético.

Silveira e Faleiros Júnior (2024) documentam exemplarmente essa tensão ao analisar a recriação da cantora Elis Regina em campanha publicitária automobilística: a ausência de autorização dos herdeiros e a exploração comercial da identidade, da voz e da imagem da artista falecida configuram violações jurídicas autônomas que a simples rotulagem do conteúdo como gerado por IA não teria o condão de afastar. O caso ilustra que a rotulagem informa, mas não autoriza; indica a artificialidade, mas não sana a ilegitimidade do uso dos atributos da personalidade.

Uma dimensão particularmente grave situa-se nos *deepfakes* de conteúdo íntimo e sexualmente explícito. Citron e Franks (2014) demonstraram, em análise pioneira sobre a criminalização da pornografia de vingança, que a distribuição não consentida de conteúdo sexualmente

explícito representa violação grave da privacidade sexual e da dignidade da pessoa retratada. Quando o conteúdo íntimo é sinteticamente fabricado por IA, sem qualquer participação real da pessoa retratada, o desvalor da conduta é potencialmente ainda maior, pois não existe sequer o registro original: trata-se de uma fabricação completa da sexualidade e da intimidade da vítima. Nesses casos, a rotulagem não apenas é insuficiente para afastar a ilicitude, como se revela evidência adicional de que o produtor e o distribuidor tinham plena consciência do caráter artificial e não consentido do material.

A LGPD reforça essa perspectiva sempre que o conteúdo sintético envolver dados biométricos de pessoa identificável. Os atributos faciais, vocais e corporais utilizados para o treinamento de modelos generativos ou para a síntese do conteúdo final qualificam-se como dados pessoais sensíveis (art. 5.º, II), cuja operação exige consentimento específico e destacado (art. 11, I) ou outra base legal expressamente prevista. A mera rotulagem do produto final não satisfaz as exigências de base legal para o tratamento de dados pessoais na fase de treinamento, coleta ou síntese.

4.2. Publicidade sintética, falsa autenticidade e enganosidade

O segundo campo de limites da rotulagem situa-se na publicidade. Em contextos comerciais, a rotulagem do conteúdo como sintético não afasta a enganosidade quando a mensagem produz falsa impressão de endosso, experiência real, recomendação humana, aprovação espontânea ou autenticidade da comunicação persuasiva.

O art. 37 do Código de Defesa do Consumidor proíbe toda publicidade enganosa, assim compreendida aquela que contenha informação ou comunicação capaz de induzir o consumidor ao erro a respeito de qualquer elemento essencial do produto ou serviço oferecido (§ 1.º). A publicidade é enganosa também por omissão, quando deixar de informar sobre dado essencial do produto ou serviço (§ 3.º). Quando um conteúdo sintético cria a

falsa impressão de que uma celebridade endossou determinado produto, de que um consumidor real relatou sua experiência, ou de que uma recomendação humana autêntica está sendo feita — e o rótulo "gerado por IA" não é suficientemente perceptível para desfazer essa impressão no consumidor médio —, configura-se publicidade enganosa, independentemente da existência formal do rótulo.

A ostensividade do rótulo é, portanto, critério central de conformidade. Um rótulo que atenda apenas formalmente ao dever de informação, mas seja periférico, minúsculo, de baixo contraste visual, em idioma técnico inacessível, ou exibido por tempo insuficiente para ser percebido, não satisfaz a exigência de clareza e ostensividade dos arts. 31 e 37 do CDC. A responsabilidade pela conformidade recai sobre o anunciante, o agente de publicidade e, em certas circunstâncias, sobre a plataforma distribuidora, conforme o papel de cada agente na cadeia de produção e veiculação do conteúdo.

A publicidade velada constitui risco específico dos influenciadores virtuais e dos avatares sintéticos. O art. 36, caput, do CDC exige que toda publicidade seja clara e ostensivamente identificada como tal. Quando um influenciador virtual interage com consumidores em redes sociais sem revelar sua natureza artificial e seu vínculo comercial com o anunciante, viola simultaneamente o dever de identificação publicitária e o dever de informação sobre a natureza do comunicador. Gasparatto, Freitas e Efig (2019, p. 78) fundamentam a responsabilidade objetiva dos influenciadores digitais no art. 14 do CDC, por defeito no serviço de informação prestado ao consumidor; o mesmo raciocínio se aplica aos operadores de influenciadores virtuais, que assumem posição funcional de fornecedoras no mercado de consumo, sujeitando-se aos deveres de informação, identificação publicitária, transparência e não enganabilidade próprios do regime consumerista.

A dimensão da vulnerabilidade algorítmica estrutural do consumidor digital merece atenção especial. Verbicaro e Vieira (2021, p. 208) demonstram

que a captação, o tratamento e a difusão de dados pessoais por dispositivos dotados de inteligência artificial criam condição estrutural de assimetria informacional que se soma à vulnerabilidade inerente do consumidor. Com efeito, a combinação entre perfilamento comportamental por *big data* e publicidade direcionada cria condições para práticas abusivas voltadas a grupos hipervulneráveis, incluindo crianças, idosos e pessoas em situação de vulnerabilidade situacional, com potencial configuração de publicidade abusiva nos termos do art. 37, § 2.º, do CDC, ainda que a natureza sintética do conteúdo seja formalmente revelada (Rosa; Faleiros Júnior; Versiani, 2020).

Em ambientes de publicidade digital altamente personalizados, o rótulo perde progressivamente sua função informacional. O consumidor repetidamente exposto a conteúdo sintético de alta qualidade, em volume elevado, com curadoria algorítmica e velocidade de circulação que impede verificação individual, não está em condição de exercer vigilância eficaz apenas com base na presença formal de um rótulo. A rotulagem, nesse contexto, deve ser complementada por mecanismos estruturais de governança, rastreabilidade e educação digital que permitam ao consumidor reconhecer, avaliar e contestar o conteúdo sintético de modo efetivo.

4.3. Plataformas, monetização e responsabilidade civil

O terceiro campo de limites da rotulagem envolve a responsabilidade das plataformas digitais que hospedam, recomendam, monetizam ou amplificam conteúdo sintético danoso. A complexidade desse campo decorre da diversidade funcional das plataformas e da necessidade de superar análises que as tratam de modo homogêneo como intermediários passivos.

O art. 19, *caput*, do Marco Civil da Internet estabelece a regra geral de que os provedores de aplicações de internet somente serão responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros se, após

ordem judicial específica, não tomarem as providências para tornar indisponível o conteúdo apontado como infringente. Essa proteção, concebida para incentivar a hospedagem de conteúdo e preservar a liberdade de expressão, não pode ser lida como cláusula geral de imunidade quando a plataforma transcende a função de hospedeira passiva.

Barbosa (2022, p. 797) demonstra que as plataformas digitais podem ocupar múltiplas posições jurídicas — provedoras de infraestrutura, operadoras de marketplace, intermediárias de serviços —, e que sua exposição à responsabilidade varia conforme o papel efetivamente exercido. Quando a plataforma recomenda, monetiza, segmenta, impulsiona ou integra conteúdo sintético a uma cadeia econômica de publicidade digital, seu envolvimento na circulação do dano vai além da mera hospedagem. Nesses casos, o regime de responsabilidade objetiva pelo risco da atividade (art. 927, parágrafo único, do Código Civil) e a responsabilidade por defeito do serviço (art. 14 do CDC) apresentam fundamentos mais adequados para a imputação de responsabilidade do que o regime de responsabilidade subjetiva por omissão após notificação judicial. A distinção entre hospedar passivamente conteúdo de terceiro e recomendá-lo, segmentá-lo, monetizá-lo, impulsioná-lo ou integrá-lo a uma cadeia econômica é, portanto, decisiva para a análise da responsabilidade civil.

A lógica do *Digital Services Act*, Regulamento (UE) 2022/2065, é ilustrativa nesse sentido. Os arts. 34 e 35 do DSA impõem às plataformas de grande porte deveres de avaliação e mitigação de riscos sistêmicos, incluindo riscos relacionados à disseminação de desinformação, conteúdo ilícito e conteúdo gerado ou manipulado por IA. Essa abordagem sistêmica é preferível à imunidade genérica fundada na ausência de conhecimento específico do conteúdo, especialmente quando a plataforma participa da monetização e da amplificação algorítmica do conteúdo danoso.

Em hipóteses de tratamento massivo e inadequado de dados pessoais, o dano moral coletivo pode assumir caráter autônomo, fundado na violação

sistemática de direitos da personalidade de grupo determinado ou determinável (Teixeira Neto; Faleiros Júnior, 2021, p. 268). Essa lógica pode ser transposta para os contextos de disseminação sistêmica de conteúdo sintético danoso: quando a plataforma falha em adotar mecanismos de governança, rotulagem, restrição ou desmonetização de conteúdo sintético lesivo, pode responder tanto por danos individuais quanto por dano moral coletivo, com fundamento nos arts. 6.º, VI, e 81 do Código de Defesa do Consumidor.

A responsabilidade civil pelo conteúdo sintético danoso pode, portanto, ser imputada de modo cumulativo aos diferentes agentes da cadeia: o produtor do conteúdo, que utiliza IA de modo não autorizado ou enganoso; o anunciante, que contrata e economicamente se beneficia da comunicação; a plataforma, que distribui, recomenda e monetiza; e o operador do sistema de IA, quando houver defeito no produto ou no serviço. Os arts. 7.º, parágrafo único, e 34 do CDC, ao lado dos arts. 186, 187 e 927 do Código Civil, oferecem a base normativa para essa responsabilização solidária e proporcional. A rotulagem adequada — quando efetivamente implementada como arquitetura de transparência, e não como mero cumprimento formal — pode ser relevante para a aferição da boa-fé, do nexo causal e da culpa em eventual ação de responsabilidade civil. A ausência dessas medidas, ao contrário, constitui indício de negligência ou de omissão dolosa na gestão dos riscos inerentes ao uso comercial da inteligência artificial generativa.

5. Conclusão

A análise desenvolvida permite confirmar a hipótese central do artigo. A rotulagem de conteúdo sintético deve ser reconhecida como dever jurídico autônomo de transparência, construído a partir da boa-fé objetiva, do dever de informação, da proteção da confiança, da tutela do consumidor, da proteção de dados pessoais e das exigências contemporâneas de governança

algorítmica. No contexto da inteligência artificial generativa, a identificação da natureza sintética do conteúdo não é mera recomendação ética ou providência facultativa de autorregulação. Ela constitui mecanismo mínimo de recomposição da assimetria informacional produzida por tecnologias capazes de fabricar aparência de realidade, autoria, presença, voz, identidade ou endosso.

Esse dever, contudo, possui função juridicamente limitada. A rotulagem torna visível a artificialidade, mas não purifica a ilicitude. Quando o conteúdo sintético utiliza imagem, voz, nome, identidade pessoal, dados biométricos ou atributos reputacionais de pessoa real, a informação de que houve emprego de IA não substitui o consentimento nem afasta a incidência dos direitos da personalidade. Do mesmo modo, em contextos comerciais e publicitários, o rótulo não elimina a enganosidade se a comunicação cria falsa impressão de endosso, experiência real, recomendação humana, neutralidade da mensagem ou autenticidade da comunicação persuasiva. A suficiência da informação deve ser aferida à luz de sua clareza, ostensividade, posição, inteligibilidade e efetiva capacidade de ser percebida pelo consumidor médio.

A licitude do conteúdo sintético depende, portanto, de uma articulação normativa mais ampla. A rotulagem deve ser combinada com consentimento válido quando houver exploração de atributos da personalidade; base legal adequada e observância dos princípios da LGPD quando houver tratamento de dados pessoais; respeito às regras consumeristas de identificação publicitária, não enganosidade e proteção contra abusos; e responsabilidade civil dos agentes que produzem, contratam, distribuem, monetizam, impulsionam ou amplificam o conteúdo danoso. No caso das plataformas, a análise não pode se limitar à categoria abstrata do intermediário. É indispensável verificar o papel concretamente desempenhado: hospedar passivamente conteúdo de terceiro é diferente de recomendá-lo, segmentá-lo, monetizá-lo, impulsioná-lo ou integrá-lo a uma cadeia econômica de publicidade digital.

O modelo regulatório adequado deve, por isso, superar a concepção reducionista de rotulagem como simples aviso textual. A transparência de conteúdo sintético exige uma arquitetura composta por sinais visíveis ao usuário, metadados, credenciais de conteúdo, mecanismos de proveniência, rastreabilidade técnica, verificabilidade, classificação por risco, *accountability* e deveres proporcionais ao papel de cada agente. Ainda assim, tais instrumentos não esgotam o juízo de licitude. São ferramentas de governança e prova, não autorizações gerais para explorar identidade, imagem, voz ou confiança.

A reconstrução dogmática proposta conduz a uma conclusão central: a rotulagem é indispensável para tornar visível a artificialidade, mas insuficiente para tornar lícito aquilo que permanece abusivo, enganoso ou lesivo à personalidade.

Referências

- AJDER, Henry; PATRINI, Giorgio; CAVALLI, Francesco; CULLEN, Laurence. **The state of deepfakes: landscape, threats, and impact**. Amsterdã: Deepttrace, 2019. Disponível em: https://regmedia.co.uk/2019/10/08/deepfake_report.pdf. Acesso em: 25 maio 2026.
- ALVES, Fabrício Germano; MOURA, Gabriel Lins Procópio de; GOMES, Lucas Quirino. Limites jurídicos da utilização da imagem de atletas em jogos eletrônicos. **Revista do Curso de Direito da UNIFOR-MG**, Formiga, v. 13, n. 2, p. 152-194, jul./dez. 2022.
- BARBOSA, Mafalda Miranda. Responsabilidade civil das plataformas digitais. **Revista de Direito da Responsabilidade**, Coimbra, ano 4, p. 791-810, 2022.
- BORGES, Gustavo; MELLO FILHO, Ricardo de Souza. Inteligência artificial generativa e os impactos nas relações de consumo. **Revista de Direito do Consumidor**, São Paulo, v. 32, n. 149, p. 279-300, set./out. 2023.
- BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 2.338/2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Câmara dos Deputados, 2025. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>. Acesso em: 25 maio 2026.
- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 maio 2026.
- BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Brasília: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 25 maio 2026.
- BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. **Código Civil**. Brasília: Presidência da República, 2002. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 25 maio 2026.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 25 maio 2026.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 25 maio 2026.

CHESNEY, Robert; CITRON, Danielle Keats. Deep fakes: a looming challenge for privacy, democracy, and national security. **California Law Review**, Berkeley, v. 107, p. 1753-1819, 2019. Disponível em: https://scholarship.law.bu.edu/faculty_scholarship/640/. Acesso em: 25 maio 2026.

CITRON, Danielle Keats; FRANKS, Mary Anne. Criminalizing revenge porn. **Wake Forest Law Review**, Winston-Salem, v. 49, p. 345-391, 2014. Disponível em: https://scholarship.law.bu.edu/faculty_scholarship/643/. Acesso em: 25 maio 2026.

COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY. **C2PA: verifying media content sources**. [S. l.]: C2PA, 2026. Disponível em: <https://c2pa.org/>. Acesso em: 25 maio 2026.

CONTENT CREDENTIALS. **Verify media authenticity**. [S. l.]: Content Credentials, 2026. Disponível em: <https://contentcredentials.org/>. Acesso em: 25 maio 2026.

GASPARATTO, Ana Paula Gilio; FREITAS, Cinthia Obladen de Almendra; EFING, Antônio Carlos. Responsabilidade civil dos influenciadores digitais. **Revista Jurídica Cesumar**, Maringá, v. 19, n. 1, p. 65-87, 2019. DOI: <https://doi.org/10.17765/2176-9184.2019v19n1p65-87>.

NATIONAL SECURITY AGENCY et al. **Strengthening multimedia integrity in the generative AI era**. [S. l.]: NSA, 2025. Disponível em: <https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF>. Acesso em: 25 maio 2026.

ROSA, Luiz Carlos Goiabeira; FALEIROS JUNIOR, José Luiz de Moura; VERSIANI, Rodrigo Luiz da Silva. A proteção do consumidor diante das práticas publicitárias abusivas realizadas por meio de big data e hipervulnerabilidade. **Revista da Faculdade Mineira de Direito**, Belo Horizonte, v. 23, n. 45, p. 235-255, 2020.

SILVEIRA, Pedro Henrique Scoralick; FALEIROS JUNIOR, José Luiz de Moura. Inteligência artificial e a exploração do direito de imagem a partir dos deepfakes. **Inova Jur — Revista Jurídica da UEMG**, Belo Horizonte, v. 3, n. 2, p. B1-19, jul./dez. 2024. ISSN 2965-6885.

TEFFÉ, Chiara Spadaccini de. Direito à imagem na internet: estudo sobre o tratamento do Marco Civil da Internet para os casos de divulgação não autorizada de imagens íntimas. **Revista de Direito Civil Contemporâneo**, São Paulo, p. 93-127, 2018.

TEIXEIRA NETO, Felipe; FALEIROS JUNIOR, José Luiz de Moura. Dano moral coletivo e vazamentos massivos de dados pessoais: uma perspectiva luso-brasileira. **Revista de Direito da Responsabilidade**, Coimbra, ano 3, p. 265-287, 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE, **Digital Services Act**. Jornal Oficial da União Europeia, Bruxelas, 27 out. 2022. Disponível em: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>. Acesso em: 25 maio 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Estabelece regras harmonizadas em matéria de inteligência artificial. **Jornal Oficial da União Europeia**, Bruxelas, 12 jul. 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>. Acesso em: 25 maio 2026.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**, São Paulo, p. 195-226, 2021.

Artigo recebido em: 25/05/2026.

Aceito para publicação em: 10/08/2026.