EPIC 2025
XII ENCONTRO DE PESQUISA, XVI ENCONTRO DE INICIAÇÃO CIENTÍFICA E
II ENCONTRO DE ENSINO E EXTENSÃO UNIVERSITÁRIA

INTELIGÊNCIA ARTIFICIAL E RESPONSABILIZAÇÃO PENAL: O DESAFIO JURÍDICO DOS DEEPFAKES

Leticia Gioia Diniz[1]
Diego Oliveira[2]
Laura de Melo Pedroso[3]
Sabrina Stramaro Sembarski[4]

Resumo: As *deepfakes* são mídias com simulações reais, mas que podem ser usadas para meios ilícitos com o objetivo de fraudes a usuários inocentes. Este artigo tem por objetivo geral, analisar os desafios jurídicos da responsabilização penal, considerando tanto o criador da tecnologia quanto o usuário que manipula a mídia,o estudo adota como método o uso de referências bibliográficas,estudos científicos e estudos de caso com uma abordagem qualitativa. Ainda, por objetivo específico esclarecer o que são as deepfakes, identificar os riscos que essa nova tecnologia traz, analisar se a responsabilização penal deve cair sobre o criador da tecnologia ou o usuário, ou ambos e propor reflexões críticas sê o avanço da inteligência artificial pode trazer novos desafios penais. A pesquisa está em busca de aprofundar quem deve ser responsabilizado penalmente pelo uso criminoso de deepfakes: o criador da tecnologia, o usuário que manipula a mídia ou ambos?

Palavras-chave: Deepfakes; Inteligência Artificial; Uso indevido.

Abstract: Deepfakes are media that simulate real life, but they can be used for illicit purposes to defraud innocent users. The general objective of this article is to analyze the legal challenges of criminal liability, considering both the creator of the technology and the user who manipulates the media. The study uses bibliographical references, scientific studies, and case studies with a qualitative approach. Furthermore, the specific objective is to clarify what deepfakes are, identify the risks this new technology poses, analyze whether criminal liability should fall on the creator of the technology or the user, or both, and propose critical reflections on whether the advancement of artificial intelligence may pose new criminal challenges. The research seeks to further understand who should be held criminally responsible for the criminal use of deepfakes: the creator of the technology, the user who manipulates the media, or both?

[1] Professora do curso de direito, pela UNIFATEB, campus Telêmaco Borba – e-mail: <leticiagioia@hotmail.com>.
[2] Graduando do curso de direito da UNIFATEB, campus Telêmaco Borba – e-mail: <diegoef11@gmail.com>.
[3] Graduanda do curso de direito, pela UNIFATEB, campus Telêmaco Borba – e-mail: <lauramelo911@gmail.com>.
[4] Graduanda do curso de direito da UNIFATEB, campus Telêmaco Borba – e-mail: <sembarski.sabrina@gmail.com>.

Key-words: Artificial Intelligence; Deepfakes; Improper Use.

1. INTRODUÇÃO

A Inteligência Artificial (IA) deixou de ser apenas uma ideia de futuro e passou a estar presente em tudo que fazemos no nosso dia a dia. Seja em ferramentas simples de trabalho, comunicação, lazer ou até mesmo trabalhos mais complexos. No passado era impensável fazermos tudo que se faz com as soluções de inteligência artificial. As soluções alcançadas com IA trazem benefícios inegáveis, mas também podem trazer sérias preocupações de onde tudo isso pode chegar.

Muito tem se falado sobre os perigos da IA no mundo e como podem, inclusive, substituir trabalhadores nos postos de trabalho, além disso também já se fala na IAG, Inteligência Artificial Geral que pode aprender e raciocinar e se adaptar a qualquer área de sabedoria dos humanos trazendo possíveis riscos a humanidade por possíveis erros de interpretação ou automação exagerada.

É muito importante reforçar os benefícios da IA em usos práticos. Os principais benefícios se destacam na eliminação de atividades repetitivas, aumentando a eficiência e redução na prática de algumas atividades, aceleração e customização do aprendizado em diversas áreas do conhecimento. Desenvolvimento de pesquisas e toda geração de renda possível a partir de negócios relacionados à inteligência artificial.

Segundo Brynjolfsson, Li e Raymond (2023) a IA tem gerado ganhos expressivos em eficiência, por exemplo, trabalhadores experientes podem aumentar em 40% seu resultado com uso de IA. E resultados melhores não são vistos somente para grandes empresas e locais extremamente organizados, estudos mostram que pequenas empresas também podem aumentar em até 20% a produtividade dos pequenos negócios (The Times, 2024).

Como podemos observar, é inquestionável a série de benefícios que a IA pode trazer para a sociedade atual e forem usadas de forma adequada e para bom propósito.

Em oposição aos benefícios, percebemos alguns riscos que podem trazer diversos prejuízos a pessoas inocentes, que acabam caindo em fraudes, ciladas e até mesmo agentes criminosos que estão tentando se beneficiar através da hipossuficiência intelectual dos usuários, com uso de tecnologia de IA.

Um exemplo claro disso são as *deepfakes*, que são mídias que simulam a realidade humana de maneira muito eficiente. Muitas vezes confundido as pessoas por acharem que se trata de uma pessoa real falando atráves das midias sociais, podendo inclusive ser usado por práticas criminosas, como roubo, pornografia, fraudes e manipulação da sociedade como um todo.

Além dos possíveis prejuízos financeiros, num mundo cada vez mais focado na individualidade, esse tipo de uso pode causar mais afastamento das pessoas e intensificação da desconfiança geral. Sem falar nas questões emocionais e psicológicas que pessoas enganadas podem sofrer além do impacto nos familiares próximos.

Outro ponto importante, nesse contexto, é o aumento da falta de credibilidade das plataformas de mídias sociais, estudos apontam que quanto mais *deepfakes* existirem maior será o desuso das redes sociais, trazendo inclusive prejuízo às próprias plataformas. Essa quebra na credibilidade não afeta somente a confiança nas informações mas impacta diretamente a importância das redes sociais.

Nesse sentido, o direito tem um desafio complexo de identificar culpados por esse tipo de manipulação, passando desde o processo de reconhecimento da fraude, registro, tratamento e posterior identificador dos causadores do impacto. É muito importante lembrar que muitas vezes o nível de qualificação da sociedade e nível de desinformação pode dificultar ainda mais o reconhecimento adequado das situações.

A importância dessa pesquisa está em discutir no âmbito penal e social as possibilidades de contornar essas variáveis que margeiam a vida de cada um no contexto social atual. No âmbito social a discussão se diz muito em como desenvolver a os usuários para se manterem cada vez mais atentos e preparados para se depararem com situações desconfortáveis. No âmbito jurídico a discussão vai se dar em como gerar mais repertórios para possibilidades legislativas que possam preencher lacunas no direito atual.

Com isso, o objetivo principal desse trabalho é analisar o desafio da responsabilização penal do uso ilícito de *deepfakes* no ordenamento jurídico brasileiro, abordando o ponto de vista das plataformas de tecnologia e também o ponto de vista do usuário que manipula a mídia. Complementando, ainda, temos como objetivo específico conceituar as *deepfakes*, identificar os possíveis danos que essa tecnologia pode trazer e analisar quem é o responsável penal pelas fraudes e prejuízos causados pela *deepfakes*.

2. DESENVOLVIMENTO

2.1 INTELIGÊNCIA ARTIFICIAL, DEEPFAKES E INOVAÇÃO TECNOLÓGICA

Diferente do que muitos pensam, a IA não surgiu recentemente. Em 1950 McCulloch e Pitts desenvolveram o primeiro modelo de rede neural artificial sendo considerado a base para os estudos futuros, poucos anos depois, em 1956, o termo “Inteligência Artificial” foi oficialmente utilizado por John McCarthy na Conferência de Dartmouth, marco fundador da área. E algum tempo depois a IA teve uma grande visibilidade com o supercomputador Deep Blue, da IBM em 1997 onde derrotou o campeão mundial de Xadrez, provando o potencial da tecnologia.

Conforme o passar dos anos as tecnologias apenas evoluíram, tornando-se possível que deepfakes possuem a capacidade de criação de conteúdos sintéticos altamente realistas. O aumento do poder computacional, principalmente com o uso de placas gráficas (GPUs) e serviços de computação em nuvem, permitiu o treinamento de modelos de grande porte, somado a isso, a ampla disponibilidade de dados em redes sociais e bancos de imagens forneceu material em abundância para o aprendizado das máquinas.

Atualmente, o Brasil tem recorde nas tentativas de fraude financeira. Segundo levantamento da Serasa Experian (2025), foram mais de 1,2 milhões de ocorrências desde janeiro, o que representa a ação de golpistas a cada 2,2 segundos no país.

Os golpes são facilmente aplicados por meio das redes sociais. Golpistas se passando por colegas, parentes, ou até mesmo prestadores de serviços, assim além de realizarem uma conversa é possível mandar áudio e ligação por vídeo o que

transmite confiança a vítima fazendo com que acredite que não se trata de golpes e sim conhecidos com dificuldades.

Apesar dos vídeos de IA serem muito utilizados para o marketing digital, entretenimento com vídeos humorísticos entre outros, os fins dependem das intenções e do contexto em que são aplicados, por isso é de tamanha importância investir em ferramentas de proteção digital,educação digital e novas leis que possam suprir as necessidades que vêm surgindo juntamente com os avanços tecnológicos.

2.2 IMPACTOS JURÍDICOS E SOCIAIS DAS DEEPFAKES NO BRASIL

O avanço da inteligência artificial trouxe inúmeros benefícios, mas também iniciou um cenário de diversas dificuldades e desafios em função do seu uso, com os chamados *deepfakes*. Esse tipo de mídia é manipulada digitalmente, ficando extremamente realista, com possibilidade de transformar a percepção de realidade das pessoas afetando indivíduos, instituições democráticas, e também, a própria credibilidade das plataformas digitais.

No aspecto jurídico, os *deepfakes* afetam diretamente direitos básicos garantidos pela Constituição Federal de 1988, como o direito à honra, dignidade, a privacidade e o direito da imagem. Contudo, com a inexistência de legislação específica leva ao tratamento de *deepfakes* de forma indireta, como através da lei Carolina Dieckmann e também do Marco Civil da Internet que traz normas para o uso da rede e faz registro de conexões para fins de responsabilização. Colaborando com isso, temos também o Código Penal que trata de calúnia e difamação, que podem ser aplicados aos *deepfakes* que foram usados para atrapalhar a reputação de pessoas. Todavia, tais dispositivos não foram feitos para lidar com tecnologias tão avançadas o que mostra possíveis lacunas jurídicas importantes.

Do ponto de vista social, os impactos têm sido muito graves. A Inteligência Artificial e *deepfakes* tem sido usadas em golpes financeiros, ataques a figuras públicas e uso em pornografia de vingança afetando diretamente mulheres, e impactam a sociedade brasileira no contexto de violência digital de gênero. Além desses impactos sociais, deepfakes podem ser usadas diretamente para tentativa de

manipulação de campanhas políticas e eleitorais, podendo comprometer a democracia e a confiança do povo em processos legítimos.

Outro foco relevante é o impacto de *deepfakes* na própria credibilidade das plataformas digitais. Alguns estudos apontam que quanto maior a quantidade desses conteúdos e mídias, maior a chance de perda de credibilidade nas redes sociais. Isso gera perda de segurança em até conteúdos reais e passam a ser vistos com desconfiança, isso tem sido chamado do “dividendo do mentiroso” (Schiff; Bueno, 2024). Esse impacto, não somente, quebra a confiança de todos nas plataformas digitais, mas também, pode levar a prejuízos financeiros as próprias empresas proprietárias dessas redes sociais que precisam da atenção e engajamento dos usuários.

Como pode ser observado, os impactos sociais e jurídicos de *deepfakes* no Brasil revelam a urgência de ações conjuntas que possam tratar essa situação de forma eficiente. É preciso entender que, as normas atuais não são suficientes e os prejuízos causados por essas tecnologias não são apenas individuais, mas podem afetar a democracia de um país e a própria credibilidade nas plataformas digitais.

2.3 ANÁLISE DO ORDENAMENTO JURÍDICO ATUAL E SUAS LACUNAS

Segundo Pacheco (2023, p. 16), o termo *deepfake* surgiu em 2017, apelidado por um usuário do *Reddit* (plataforma que combina as funcionalidades de um fórum de discussão com uma rede social), para postar conteúdos pornograficos alterados digitalmente com imagens de celebridades. Desde 2017, o uso dos *deepfakes* vem crescendo, seja para recreação ou uso criminoso, os impactos jurídicos do mau uso geram discussões acerca da criação de novas legislações que possam preencher as lacunas existentes.

O surgimento de novas tecnologias trouxe novos desafios à proteção dos direitos individuais e à atuação da administração pública que deve responder de forma ética e eficiente mesmo diante de lacunas. De acordo com o Art. 37 da Constituição Federal de 88, a administração pública deve basear-se nos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Esses princípios não se limitam às leis já existentes, eles exigem uma atuação atualizada e capaz de lidar com novas

tecnologias, garantindo proteção aos cidadãos e eficiência na gestão pública. Embora não existam leis existentes sobre *deepfakes*, a Constituição Federal, em seu princípio da eficiência impõe que o Estado adote medidas preventivas e regulatórias, usando legislações existentes como base, aplicando interpretação moderna.

Nesse sentido, não existem legislações que tratem especificamente de deepfakes, porém encontram-se legislações relacionadas. A lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, tipifica a invasão em dispositivos com intuito de adulterar ou destruir dados ou informações sem autorização do titular do dispositivo. Embora, essa legislação seja voltada a crimes cibernéticos em geral, pode servir como referência para relacionar práticas aos *deepfakes*, como a obtenção, alteração ou divulgação de imagens e vídeos sem consentimento do indivíduo.

Ademais, o Código Penal aborda situações onde se aplicam sanções que se enquadram no uso indevido de *deepfakes*, exemplificando, tem-se a calúnia no Art. 138, que trata sobre acusar falsamente alguém de ter cometido algum crime, o Art. 139 que diz “difamar alguém, imputando-lhe fato ofensivo à sua reputação”, ou seja quando algum indivíduo comete ato ofensivo à reputação de outrem, como algo contra sua imagem, há sanção, e a Injúria, abordada no Art. 140, que diz que ofender a dignidade ou decoro de alguém. Estes dispositivos legais, embora concebidos para proteger a honra e imagem das pessoas, não preveem explicitamente tecnologias como deepfakes. Assim, conteúdos manipulados que difamam, caluniam ou injuriam podem causar graves danos, exigindo interpretação adaptada e reflexão sobre lacunas legais.

Nesse contexto, o Marco Civil da Internet (Lei nº 12.965/2014) também se mostra relevante pois estabelece direitos e deveres no ambiente digital. O Art. 7º assegura aos usuários proteção de dados pessoais e privacidade, enquanto o Art. 10º prevê a guarda de registros de conexão, permitindo rastreabilidade em casos de abusos. Dessa forma, embora não trate especificamente de deepfakes, o Marco Civil oferece meios para responsabilização e proteção em situações envolvendo conteúdos digitais manipulados.

Diante dessas lacunas, observa-se a necessidade de aperfeiçoamento da legislação e de mecanismos de controle e rastreamento digital, capazes de responsabilizar autores de *deepfakes* ilícitas e proteger efetivamente os direitos dos indivíduos.

2.4 RESPONSABILIZAÇÃO PENAL E INOVAÇÃO NO CONTROLE NO COMBATE AO CRIME

O crescente uso de *deepfakes* gera dificuldades sobre quem deve ser responsabilizado penalmente, considerando diferentes agentes e a necessidade de inovação tecnológica para prevenção e investigação desses crimes (Alves et al., 2024; Pacheco, 2023). A manipulação digital de imagens e vídeos pode afetar a honra, a imagem e a privacidade dos indivíduos, exigindo respostas jurídicas eficazes.

Os criadores das ferramentas de *deepfake* enfrentam uma questão legal importante, embora o desenvolvimento da tecnologia não configure crime, pode haver responsabilização em caso de dolo eventual, quando o autor tinha conhecimento de que sua criação poderia ser usada para fins ilícitos (Nakanishi, 2023). Por outro lado, os usuários que produzem ou distribuem *deepfakes* com a intenção de prejudicar terceiros são responsáveis diretos pelos danos. Nesse contexto, normas sobre falsidade ideológica, crimes contra a honra (arts. 138, 139 e 140 do Código Penal) e invasão de dispositivos digitais (Lei nº 12.737/2012) podem ser aplicadas, embora ainda apresentem lacunas diante das particularidades tecnológicas dessas condutas (Medon, 2021).

As plataformas digitais possuem responsabilidade compartilhada na moderação de conteúdos, a lei do Marco Civil da Internet (Lei nº 12.965/2014) prevê que os provedores devem remover conteúdos ilícitos após notificação, mas não têm obrigação de sempre monitorar toda a atividade online (Brasil, 2014). Essa limitação busca equilibrar a liberdade de expressão e a proteção dos usuários.

Internacionalmente, observam-se diferentes abordagens. Nos Estados Unidos, o debate envolve liberdade de expressão versus responsabilidade civil e penal, com legislação específica ainda em construção. Na União Europeia, o *Digital Services Act* (DSA) estabelece regras para moderação e responsabilização das plataformas.

Além da legislação, a inovação tecnológica complementa a responsabilização penal, como técnicas de *watermarking* digital permitem identificar a origem dos vídeos, algoritmos de inteligência artificial detectam *deepfakes* automaticamente, e perícia digital avançada possibilita rastreamento da autoria (Nakanishi, 2023; Pacheco, 2023). Essas soluções não substituem a lei, mas aumentam a eficiência do Estado na prevenção, investigação e responsabilização de condutas ilícitas.

Assim, a responsabilização penal aos *deepfakes* exige uma abordagem integrada, que combine interpretação adaptativa da legislação vigente, inovação tecnológica e medidas preventivas, garantindo proteção aos direitos individuais e eficiência na atuação estatal diante das novas demandas digitais.

2.5 DESAFIOS PROBATÓRIOS E INVESTIGATIVOS

O termo *deepfake*, ainda é pouco conhecido e devido a falta de divulgação do tema as pessoas podem achar que isso não faz parte da realidade em que estão vivendo, muita das vezes se acham espertos e que jamais caíram em golpes, ainda mais aplicados por inteligência artificial.

Quanto mais a tecnologia se desenvolve mais realista e difícil de distinguir da realidade fica. Atualmente, a inteligência artificial tem sido usada em coisas inimagináveis, um bom exemplo disso seriam as eleições de 2024 onde foram postadas diversas propagandas eleitorais contendo *deepfakes*, algumas denegrindo a imagem dos candidatos e outras com textos falsos causando repúdio e prejudicando a integridade mental da vítima.

Ainda importante ressaltar que ninguém está escape desse perigo, existem casos relatados que ocorreram com pessoas civis, como o caso ocorrido no Mato Grosso no ano de 2024 onde alunos são expulsos após usar inteligência artificial para criar nudez falsos de professora e colegas em escola particular de Cuiabá, as imagens eram geradas a partir de fotos que mostravam os rostos das vítimas. Em seguida, as montagens eram compartilhadas em grupos de pornografia nas redes sociais.

As imagens eram geradas por quatro adolescentes entre 12 a 16 anos, conforme informa Portal G1 (2024), com isso causando graves consequências tanto para as colegas quanto para a professora, que além do dano moral, psicológico, calúnia gera

também um deepfake bullying, pois esse ato prejudicou as vítimas de formas inimagináveis em suas relações acadêmicas, familiares, sociais, psicológicas, trabalhistas entre outros danos que vão perdurar durante toda a vida das vítimas.

Com isso vemos que a IA está em todos os ambientes, em todas as idades, principalmente na geração Z e Alpha, que são considerados a geração da tecnologia, assim tendo grandes poderes em mãos, tanto para adquirir conhecimento quanto para causar grandes crimes.

2.6 PERSPECTIVAS FUTURAS E RECOMENDAÇÕES

Ao ver os desafios vindos juntos com os *deepfakes* no Brasil, é possível observar que o combate a essa tecnologias, não é só parte do Direito Penal, mas deve ser tratado como um aspecto multidisciplinar que envolve competências jurídicas, tecnológicas, sociais e educacionais.

No aspecto jurídico, observa-se a necessidade da criação de uma legislação focada em *deepfakes*, que trabalhe suas particularidades e defina critérios objetivos para responsabilização dos envolvidos. Essas normas devem trazer a tipificação penal para essas condutas ilícitas e até a previsão de medidas preventivas e reparatórias para essas vítimas.

No aspecto tecnológico, é importante garantir a detecção e rastreabilidade rápida de *deepakes*, para isso é necessário investir em mecanismos que identificam a manipulação digital e inserir marcas d'água em conteúdos, o que já é realidade em outros países.

No aspecto social, evidencia-se a necessidade urgente de programa de educação em mídias sociais e plataformas digitais. O Brasil precisa preparar a população para reconhecer e questionar conteúdos manipulados. Campanhas de conscientização nacional, alinhadas ao ensino escolar, que ensinem sobre a importância da segurança digital e a ética na utilização das tecnologias podem diminuir de maneira relevante os prejuízos individuais e coletivos da população.

Resumindo, para foco futuro é importante lidar com a integração de três aspectos importantes. Legislação adequada, tecnologia de identificação e prevenção e educação da população para uso consciente da tecnologia. Somente com o

alinhamento dos três pilares se alcançará soluções eficientes para proteger os direitos fundamentais e conseguir que as plataformas digitais sejam um espaço de confiança, aprendizado e interação social.

3. CONCLUSÃO

Desse modo, com o aumento de *deepfakes* no Brasil, surgem desafios complexos que ultrapassam o Direito Penal, a tecnologia e a sociedade. Embora a inteligência artificial ofereça benefícios significativos, seu uso indevido compromete a privacidade, a honra e a imagem das pessoas, além de afetar a credibilidade das plataformas digitais e ameaçar processos democráticos.

O ordenamento jurídico vigente ainda apresenta lacunas frente a essas novas tecnologias, reforçando a necessidade de legislação específica que direcione a criação, distribuição e responsabilização de conteúdos manipulados digitalmente. Ao mesmo tempo, é importante investir em novas tecnologias capazes de detectar essas *deepfakes*, rastreando e restringindo seu uso, bem como inserir a educação digital, considerando que vivemos em uma realidade em que a informação adequada pode gerar proteção social e acadêmica.

Diante desse contexto, surge o problema de pesquisa que norteia este estudo: quem deve ser responsabilizado penalmente pelo uso criminoso de deepfakes, o criador da tecnologia, o usuário que manipula a mídia ou ambos?

Portanto, este artigo tem como objetivo geral analisar os desafios jurídicos da responsabilização penal do uso criminoso de *deepfakes*, considerando tanto o criador da tecnologia quanto o usuário que manipula a mídia. Para isso, busca-se atingir os seguintes objetivos específicos: esclarecer o que são as *deepfakes*; identificar os riscos que essa nova tecnologia traz atualmente; analisar se a responsabilização penal deve recair sobre o criador da tecnologia, o usuário ou ambos; e propor reflexões críticas sobre como o avanço da inteligência artificial pode trazer novos desafios penais.

Assim, a combinação de normas claras, inovação tecnológica e conscientização social se apresenta como caminho indispensável para enfrentar os

riscos associados às *deepfakes* e garantir uma sociedade digital mais segura e responsável.

REFERÊNCIAS

ALVES, Bruno Moraes; ARAÚJO, Ana Karen Vasconcelos; CAVALCANTE, Juan Fonteles; GALDINO JÚNIOR, Francisco Expedito; RODRIGUES, Luiz Henrique Lopes. Análise da responsabilização criminal dos criadores e propagadores de “deep fakes” no ordenamento jurídico brasileiro. Caderno Pedagógico, v. 21, n. 6, p. 75-88, 2024. DOI: https://doi.org/10.54033/cadped.v2n16-075. Disponível

em: https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348/3313 . Acesso em: 27 ago. 2025.

BRASIL. Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Art. 138. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm#art138 . Acesso em: 03 set. 2025.

BRASIL. Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Art. 139. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm#art139 . Acesso em: 03 set. 2025.

BRASIL. Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Art. 140. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm#art140 . Acesso em: 03 set. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 3 set. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm . Acesso em: 27 ago. 2025.

BRASIL. Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 03 set. 2025.

BRASIL. Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Diário Oficial da União, Brasília, 2023. Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2881712&filename=Avulso+PL+2338%2F2023 . Acesso em: 9 set. 2025.

BRYNJOLFSSON, Erik; LI, Danielle; RAY, Lindsey R. Generative AI at work. Cambridge: National Bureau of Economic Research, 2023. (NBER Working Paper, n. 31161). DOI: https://doi.org/10.3386/w31161 . Acesso em: 27 ago. 2025.

CHESNEY, Robert; CITRON, Danielle. Deep fakes: A looming crisis for national security, democracy and privacy? California Law Review, v. 107, p. 1753-1819, 2019. Disponível em: https://revista.tre-rj.jus.br/rjed/article/download/195/190/377 . Acesso em: 9 set. 2025.

COMPROVA. Saiba o que é deepfake, técnica de inteligência artificial que foi apropriada para produzir desinformação. CNN Brasil, 27 set. 2022. Atualizado em: 27 set. 2022. Disponível em: https://www.cnnbrasil.com.br/noticias/saiba-o-que-e-deepfake-tecnica-de-inteligencia-artificial-que-foi-apropriada-para-produzir-desinformacao. Acesso em: 10 set. 2025

DINIZ, P. D. B. Os desafios regulatórios e a necessidade de tutela jurídica frente à proliferação de deepfakes. Revista Tópicos, 2025. Disponível em: https://revistatopicos.com.br/artigos/os-desafios-regulatorios-e-a-necessidade-de-tutela-juridica-frente-a-proliferacao-de-deepfakes . Acesso em: 9 set. 2025.

DINIZ, P. D. B. Os limites à reconstrução digital da imagem na sociedade tecnológica. Revista Eletrônica do Curso de Direito da UFSM, v. 17, n. 3, e67299, 2022. DOI: 10.5902/198136967299. Disponível em: https://periodicos.ufsm.br/revistadireito/article/download/67299/60807/375439 . Acesso em: 9 set. 2025.

EU. Digital Services Act (DSA): exigência de medidas específicas para conteúdos gerados por IA (como deepfakes), incluindo rotulagem clara por parte das plataformas. Digital Services Act, UE, 2022–2023. Disponível em: https://www.eu-digital-services-act.com/ . Acesso em: 9 set. 2025.

EU. EU AI Act — obrigatoriedade de rotulagem de conteúdos gerados ou manipulados por IA (como deepfakes), transparência e classificação por níveis de risco. Parlamento Europeu, 19 fev. 2025. Disponível em: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence . Acesso em: 9 set. 2025.

EUROPEAN PARLIAMENT. Children and deepfakes. Think Tank – European Parliament, 3 jul. 2025. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282025%29775855 . Acesso em: 9 set. 2025.

G1 MATO GROSSO. Alunos são expulsos após usar inteligência artificial para criar nudes falsos de professora e colegas em escola particular de Cuiabá. G1, 25 set. 2024. Disponível em: https://g1.globo.com/mt/mato-grosso/noticia/2024/09/25/alunos-sao-expulsos-apos-usar-inteligencia-artificial-para-criar-nudes-falsos-de-professora-e-colegas-em-escola-particular-de-cuiaba.ghtml. Acesso em: 10 set. 2025.

LEGALE. Deepfakes e direitos de personalidade no direito brasileiro. Blog Legale, 19 jun. 2025. Disponível em: https://legale.com.br/blog/deepfakes-e-direitos-de-personalidade-no-direito-brasileiro/. Acesso em: 9 set. 2025.

MEDON, Fillipe. O direito à imagem na era das deepfakes. Revista Brasileira de Direito Civil, v. 27, n. 1, p. 251-272, 2021. DOI: https://doi.org/10.33242/rbdc.2021.01.011. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438/447. Acesso em: 27 ago. 2025.

NAKANISHI, Maria Fernanda Mugnaini. A problemática jurídica dos deepfakes: uma análise do uso da inteligência artificial na produção de provas e suas repercussões penais. 2023. Artigo (Bacharelado em Direito) – Centro Universitário de Brasília (UniCEUB), Brasília, 2023. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/17157/1/22001667.pdf. Acesso em: 27 ago. 2025.

NERY, Alexandre. A mesma tecnologia que facilita a vida de fraudadores pode ajudar a combater este tipo de crime na internet, diz especialista. Rádio Câmara (Economia Direta), Portal da Câmara dos Deputados, 28 abr. 2025, 08h00. Disponível em: https://www.camara.leg.br/radio/programas/1153531-a-mesma-tecnologia-que-facilita-a-vida-de-fraudadores-pode-ajudar-a-combater-este-tipo-de-crime-na-internet-diz-especialista/. Acesso em: 10 set. 2025.

OLIVEIRA, G. A. G. Deep fake, direitos da personalidade e o direito penal. Revista de Direito da UFSM, v. 19, 2024. Disponível em: https://periodicos.ufsm.br/revistadireito/article/download/85239/65631/435798. Acesso em: 9 set. 2025.

PACHECO, Victor Góis de Oliveira. As verdades dos profundamente falsos: um estudo semiótico sobre deepfakes nas eleições presidenciais brasileiras de 2022. 2023. Dissertação (Mestrado em Comunicação Social) – Universidade Federal de Minas Gerais, Faculdade de Filosofia e Ciências Humanas, Belo Horizonte, 2023.

REALITY DEFENDER. The State of Deepfake Regulations in 2025: What Businesses Need to Know. Reality Defender, 18 jun. 2025. Disponível em:https://www.realitydefender.com/insights/the-state-of-deepfake-regulations-in-2025-what-businesses-need-to-know . Acesso em: 9 set. 2025.

RÁDIO E TV JUSTIÇA. JJ1 - Polícia investiga alunos de escola acusados de usar IA para montar nudes de meninas. YouTube, 14 nov. 2023. 215 visualizações. Disponível em:https://www.youtube.com/watch?v=zjsjzz_67Ao. Acesso em: 10 set. 2025

SCHIFF, Kaylyn Jackson; SCHIFF, Daniel S.; BUENO, Natália S. The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? American Political Science Review, p. 1–20, 2024. DOI:10.1017/S0003055423001454.

SERASA EXPERIAN. Brasil tem recorde nas tentativas de fraude registradas em janeiro, aponta Serasa Experian. *Serasa Experian*, São Paulo, 17 abr. 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-tem-recorde-nas-tentativas-de-fraude-registradas-em-janeiro-aponta-serasa-experian. Acesso em: 9 set. 2025.

SIQUEIRA, M. de. Deepfake e privacidade: uma análise jurídica. Revista Foco, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/5679. Acesso em: 9 set. 2025.

SHIMABUKURO, Igor; LIMA, Lucas. História da inteligência artificial: quem criou e como surgiu a tecnologia revolucionária. Tecnoblog, [s.l.], [s.d.]. Atualizado em: há 7 meses. Disponível em: https://tecnoblog.net/responde/historia-da-inteligencia-artificial-quem-criou-e-como-surgiu-a-tecnologia-revolucionaria/. Acesso em: 10 set. 2025.

SIDI. PL 2338/2023: os impactos da regulamentação da inteligência artificial no Brasil. São Paulo: SIDI, 12 dez. 2024. Disponível em: https://www.sidi.org.br/pt-br/blog/pl-2338/2023-os-impactos-da-regulamentacao-da-inteligencia-artificial-no-brasil . Acesso em: 9 set. 2025.

THE TIMES. It is not replacing people, it is supercharging people: Google AI pilot shows 20% productivity boost for small businesses. Londres: The Times, 2024. Disponível em:https://www.thetimes.co.uk/article/it-is-not-replacing-people-it-is-supercharging-people-enterprise-network-3j3r6mggq . Acesso em: 9 set. 2025.

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL (TRE-RS). Recurso Eleitoral n. 0600064-11.2024.6.21.0071, Gravataí-RS. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tre-rs/2718076132 . Acesso em: 10 set. 2025.

WEF – WORLD ECONOMIC FORUM. How can we combat the worrying rise in deepfake content? 19 de maio de 2023. Disponível em: https://www.weforum.org/stories/2023/05/how-can-we-combat-the-worrying-rise-in-deepfake-content/ . Acesso em: 9 set. 2025.