

DEEPPAKES E RESPONSABILIDADE PENAL: UMA ANÁLISE DA PRÁTICA E DA RESPONSABILIZAÇÃO NO CONTEXTO BRASILEIRO

DEEPPAKES AND CRIMINAL RESPONSIBILITY: AN ANALYSIS OF PRACTICE AND RESPONSIBILITY IN THE BRAZILIAN CONTEXT

Maria Luisa Farias Motão¹
Leonardo Silva de Oliveira Bandeira²

MOTÃO, Maria Luisa Farias; BANDEIRA, Leonardo da Silva de Oliveira. **Deepfakes e Responsabilidade Penal: Uma Análise da Prática e da Responsabilização no Contexto Brasileiro**. 21 páginas. Trabalho de Conclusão de Curso de graduação em Direito – Centro Universitário UNINORTE, Rio Branco. 2025.

RESUMO

Introdução. O presente estudo trata do avanço da tecnologia *deepfake*, baseada em inteligência artificial, e seus reflexos no Direito Penal brasileiro, com ênfase nos desafios para a responsabilização de seus criadores e propagadores. **Objetivo.** Diante desse contexto, procedeu-se ao estudo da responsabilidade penal decorrente do uso de *deepfakes*, analisando a suficiência da legislação vigente e investigando a solução dogmática mais adequada para a punição de tais condutas, seja pela criação de um novo tipo penal ou pela adaptação dos crimes existentes. **Método.** Através de embasamento teórico-bibliográfico e documental, produziu-se uma análise acerca da subsunção dos atos praticados com *deepfakes* aos tipos penais previstos no ordenamento pátrio, utilizando-se do método dedutivo. **Resultados.** O surgimento dos *deepfakes* como instrumento do crime evidenciou a possibilidade de seu enquadramento em delitos já existentes, como os crimes contra a honra, a dignidade sexual e o estelionato. No entanto, destacou-se a insuficiência da sanção atual diante do potencial lesivo da tecnologia, o que gera uma sensação de impunidade e uma proteção deficiente às vítimas. **Conclusão.** Dessa forma, conclui-se que a criação de um tipo penal autônomo para a prática de *deepfake* se mostra ineficiente e fadada à obsolescência. A solução mais adequada e proporcional consiste na inserção de uma qualificadora ou causa de aumento de pena nos crimes já tipificados, de modo a punir com maior rigor as condutas que se valem dessa tecnologia, sem inflar desnecessariamente a legislação penal.

Palavras-chave: *deepfakes*; responsabilidade penal; crimes cibernéticos; direito digital; Inteligência Artificial.

¹ Discente do 9º período do curso de bacharelado em Direito pelo Centro Universitário Uninorte.

² Docente do Centro Universitário Uninorte. Advogado, sócio do Casas, Ricardo, Bandeira & Soares Advocacia, Coordenador do Núcleo de Educação a Distância da Uninorte, Professor, especialista em Direito Civil, Docência do Ensino Superior e Legal Operations: Dados, Inteligência Artificial e Performance Jurídica pela PUC/PR.

ABSTRACT

Introduction. This study addresses the advancement of deepfake technology, based on artificial intelligence, and its repercussions on Brazilian Criminal Law, with an emphasis on the challenges for the accountability of its creators and propagators. **Objective.** In this context, the study of criminal liability arising from the use of deepfakes was conducted, analyzing the sufficiency of the current legislation and investigating the most appropriate dogmatic solution for punishing such conduct, whether through the creation of a new criminal type or the adaptation of existing crimes. **Method.** Through a theoretical-bibliographical and documentary foundation, an analysis was produced regarding the subsumption of acts practiced with deepfakes under the criminal types provided for in the national legal system, using the deductive method. **Results.** The emergence of deepfakes as a criminal instrument highlighted the possibility of its classification under existing offenses, such as crimes against honor, sexual dignity, and fraud. However, the insufficiency of the current sanction was noted, given the technology's harmful potential, which generates a sense of impunity and deficient protection for victims. **Conclusion.** Therefore, it is concluded that the creation of an autonomous criminal type for the practice of deepfake proves to be inefficient and doomed to obsolescence. The most appropriate and proportional solution consists of inserting a qualifier or a penalty enhancement clause into already typified crimes, in order to more severely punish conducts that use this technology, without unnecessarily inflating criminal legislation.

Keywords: deepfakes; criminal liability; cybercrimes; digital Law; Artificial Intelligence.

INTRODUÇÃO

A sociedade atual vivencia a Quarta Revolução Industrial, um período de transformações exponenciais impulsionado pela convergência de tecnologias digitais, físicas e biológicas, onde a inteligência artificial se destaca como protagonista. Nesse cenário de intensa digitalização das relações humanas, emerge uma nova dimensão de existência, que, ao mesmo tempo em que oferece inúmeros benefícios, se consolida como um terreno fértil para a proliferação de novas e sofisticadas práticas delitivas.

Dentre as inovações tecnológicas que mais têm levantado debates éticos, sociais e jurídicos, destaca-se a *deepfake*, uma técnica que utiliza a aprendizagem profunda (*deep learning*) para criar e manipular conteúdos audiovisuais com um grau de realismo impressionante, tornando-se cada vez mais difícil distinguir o real do sintético.

Esse fenômeno originou-se em campos da indústria cinematográfica e da sátira, essa tecnologia rapidamente transbordou para usos inquestionavelmente

ilícitos, ao realizar ações capazes de fundir imagens e vozes para criar situações que jamais ocorreram, o que abriu um leque de possibilidades maliciosas, que vão desde a disseminação de desinformação e a manipulação de processos democráticos até a prática de fraudes, crimes contra a honra e, de forma especialmente alarmante, a criação de pornografia não consensual como uma nova e cruel ferramenta de violência de gênero.

A proliferação de *deepfakes* representa, portanto, uma ameaça direta a direitos da personalidade, como a imagem, a honra, a privacidade e a própria dignidade da pessoa humana, bens jurídicos de máxima importância para o ordenamento pátrio.

Diante dessa nova realidade, que instaura uma crise de confiança na prova audiovisual e potencializa os danos às vítimas, a presente monografia se propõe a investigar o seguinte problema de pesquisa: de que forma o ordenamento jurídico-penal brasileiro responde à ameaça dos *deepfakes*, e seria a criação de um tipo penal autônomo a solução mais adequada, ou a adaptação dos crimes existentes por meio de qualificadoras se mostra mais eficiente e dogmaticamente correta?

O objetivo geral deste trabalho é, portanto, analisar a responsabilidade penal decorrente da criação e disseminação de *deepfakes* no contexto brasileiro e, foram traçados os seguintes objetivos específicos:

- a) contextualizar o fenômeno *deepfake* no âmbito dos crimes cibernéticos, explorando seus conceitos e evolução;
- b) examinar a subsunção das condutas praticadas com o uso de *deepfakes* aos tipos penais já existentes no Código Penal, notadamente os crimes contra a honra, contra a dignidade sexual e o estelionato;
- c) analisar o dilema legislativo entre a criação de um novo tipo penal e a inserção de uma qualificadora, defendendo a solução que se mostra mais proporcional e eficaz para a proteção dos bens jurídicos tutelados.

Para alcançar tais objetivos, a metodologia empregada foi a qualitativa, com procedimento técnico bibliográfico e documental, valendo-se da análise de livros, artigos científicos, notícias e da legislação pertinente às searas do Direito Penal e do Direito Digital.

O trabalho foi estruturado em três capítulos, o primeiro apresenta o panorama da criminalidade na era digital, conceituando os crimes cibernéticos e introduzindo a tecnologia *deepfake*, sua evolução e seu potencial disruptivo. O segundo capítulo

analisa a dogmática da responsabilização penal, demonstrando como as condutas maliciosas praticadas por meio de *deepfakes* se amoldam a diversos tipos penais vigentes e detalhando a pluralidade de danos causados às vítimas.

Por fim, o terceiro capítulo enfrenta a questão da resposta legislativa, discutindo a tensão entre os princípios da proteção deficiente e da legalidade, argumentando contra a criação de um tipo penal autônomo e defendendo a inserção de uma qualificadora como a solução mais adequada e juridicamente sólida para o ordenamento brasileiro.

1 CRIMES CIBERNÉTICOS

1.1 CRIMES CIBERNÉTICOS: CONCEITO, CARACTERÍSTICAS E CLASSIFICAÇÕES DOUTRINÁRIAS.

Vivemos em uma era de transformações, um período que a literatura convencionou chamar de Quarta Revolução Industrial (Schwab, 2016). Essa nova fase, protagonizada pela inteligência artificial e por softwares cada vez mais complexos, não apenas alterou os modos de produção, mas remodelou profundamente o próprio tecido social.

A digitalização das relações humanas deu origem a uma nova dimensão de existência, um ciberespaço onde as fronteiras entre o humano e a máquina se tornam cada vez mais tênues (Lima Filho, 2021). Nesse novo e fértil terreno para as interações, emergiu também, de forma inevitável, um novo campo para as práticas delitivas, dando origem ao fenômeno dos crimes cibernéticos.

Em uma primeira aproximação, pode-se conceituar o crime cibernético como toda conduta ilícita e culpável, tipificada em lei penal, que utiliza um sistema de computadores ou dispositivo eletrônico como instrumento para sua execução ou que tem como alvo a integridade, a confidencialidade ou a disponibilidade de dados e sistemas informáticos.

Com isso, podemos sintetizar esse conceito como:

Qualquer ação típica, antijurídica e culpável praticada por pessoa física ou jurídica, com o uso criminoso envolvendo processamento de dados e/ou transmissão de dados, sem a necessidade de conexão à internet. (Maues; Duarte; Cardoso, 2018, p. 171)

Para sistematizar o estudo desse fenômeno, a doutrina penal costuma classificar os crimes cibernéticos em duas categorias principais, uma distinção crucial para a correta adequação típica da conduta.

Primeiramente, temos os crimes cibernéticos próprios, também conhecidos como puros. Neles, o bem jurídico tutelado é a própria tecnologia da informação, ou seja, a conduta delituosa ataca diretamente a segurança dos sistemas. São crimes que não existiriam fora do ambiente digital.

Para melhor exemplificar, Lacerda e Silva (2021, p. 15) exemplificam condutas que podem ser consideradas crimes cibernéticos próprios ou puros: “Como crimes próprios, têm-se exemplos dos vírus que invadem os sistemas para destruir informações, roubar informações ou até mesmo danificar o aparelho, seja ele smartphones, computadores ou tablets.”

Por outro lado, encontram-se os crimes cibernéticos impróprios, ou impuros. Nessa modalidade, o sistema computacional não é o alvo, mas sim o meio, o instrumento para a prática de crimes já previstos em nosso ordenamento jurídico. A tecnologia, nesse caso, potencializa a ação de delitos tradicionais.

A esse respeito, dispõe a CPI dos Crimes Cibernéticos:

Os crimes virtuais comuns são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP - Código Penal), os crimes contra a honra (arts. 138 a 140 do CP), a veiculação de pornográfica infantil (art. 241-A do Estatuto da Criança e do Adolescente – Lei nº 8.069/90), o crime de violação ao direito autoral (art. 184 do CP), entre outros. (Brasil, 2016, p. 75)

O rol é vasto, incluindo desde o estelionato (art. 171, Código Penal) praticado via boletos falsos, os crimes contra a honra (arts. 138 a 140, Código Penal) disseminados em redes sociais, até a divulgação de cenas de estupro ou pornografia, conforme citado por Lacerda e Silva (2021, p. 15).

Alguns autores, como Lima Filho (2021), admitem ainda uma terceira categoria, a dos crimes mistos, nos quais a tecnologia é, simultaneamente, bem jurídico ofendido e meio de execução para um crime-fim.

Compreender essa distinção é fundamental, pois evidencia que o desafio do legislador e do operador do Direito não é apenas criar novos tipos penais para novas

condutas, mas também adaptar a interpretação dos tipos penais clássicos a essa nova realidade.

Ademais, no Brasil a resposta legislativa a esse fenômeno não se deu por meio de um código unificado, mas sim de forma esparsa e gradual. Atualmente, existe um conjunto de leis normativas que dialogam entre si para fundamentar a persecução penal destes tipos de crimes, destacando-se:

- a) Lei nº 12.737/2012 (Lei Carolina Dieckmann): Responsável por tipificar expressamente crimes cibernéticos próprios, notadamente a já mencionada invasão de dispositivo informático (art. 154-A, Código Penal) e a interrupção de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266, Código Penal) (Projuris, 2023);
- b) Lei nº 12.735/2012: Altera o Código Penal (Decreto-Lei nº 2.848/1940), o Código Penal Militar (Decreto-Lei nº 1.001/1969) e a Lei nº 7.716/1989 para tipificar condutas realizadas mediante o uso de sistemas eletrônicos, digitais ou similares que sejam praticadas contra sistemas informatizados e similares. Essa lei visa caracterizar e punir condutas criminosas que envolvam o uso da tecnologia digital para praticar delitos contra sistemas informatizados. Além disso, determina a estruturação de órgãos da polícia judiciária com setores e equipes especializadas no combate a crimes praticados em redes de computadores e dispositivos de comunicação ou sistemas informatizados (Migalhas, 2012);
- c) Lei nº 12.965/2014 (Marco Civil da Internet): Considerada a "constituição da internet" no país, estabelece princípios fundamentais como a neutralidade da rede, a proteção da privacidade e a liberdade de expressão (Projuris, 2024). Para a persecução penal, sua importância é imensa, pois impõe aos provedores o dever de manter registros de conexão, como o endereço de IP, ferramenta essencial para a identificação da autoria de delitos (Lima Filho, 2021);
- d) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD): Tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes (MPF, 2024).

Desta forma, a compreensão do cenário da responsabilização penal por crimes

cibernéticos no Brasil exige uma análise conjugada destes diplomas legais, aliada à aplicação do Código Penal tradicional aos novos e complexos cenários apresentados pela tecnologia.

1.2 O ADVENTO DAS DEEPFAKES: A SOFISTICAÇÃO TECNOLÓGICA DA FALSIDADE

Avançando na análise da criminalidade cibernética, é imperativo debruçar-se sobre uma das mais disruptivas e controversas tecnologias da atualidade: a *deepfake*. Palavra esta originada da junção dos termos *deep learning* (aprendizagem profunda) e *fake* (falso), descreva a manipulação de conteúdos audiovisuais por meio de sistemas de Inteligência Artificial (IA), com o propósito de criar simulações hiper-realistas, capazes de fabricar situações e discursos inteiramente novos (Faustino, 2018, p. 108).

Essa nova tecnologia, que se popularizou a partir de um usuário da plataforma Reddit (Medon, 2021), representa uma qualificação das *fake news* tradicionais.

Essa técnica eleva a desinformação a um novo patamar. Enquanto as *fake news* tradicionalmente se baseiam em textos, imagens descontextualizadas ou edições rudimentares, os *deepfakes* atacam o cerne da credibilidade da prova audiovisual, gerando um produto final cujo grau de fidedignidade é tão elevado que se torna difícil perceber a montagem (Medon, 2021, p. 262).

Ao difundir narrativas fabricadas com aparência de legitimidade, essa prática compromete severamente a confiabilidade da informação no ambiente digital (Internet Matters, 2023).

Para dimensionar o potencial lesivo dessa tecnologia, pode-se traçar um paralelo com os efeitos devastadores da desinformação em crises recentes. Durante a pandemia de COVID-19, por exemplo, a propagação de notícias falsas sobre a suposta periculosidade das vacinas contribuiu para a hesitação vacinal. O resultado dessa onda de desinformação foi trágico, impactando a saúde pública em um período em que o Brasil registrava picos alarmantes de mortalidade, como o de abril de 2021, quando a média móvel de óbitos diários se aproximava de três mil vidas perdidas (Após, 2021).

O episódio serve como um grande alerta: se textos e boatos foram capazes de causar tal dano, o que não poderia ser alcançado com um vídeo fabricado de uma autoridade sanitária ou um cientista renomado endossando teses anticientíficas?

Como adverte Pereira (2023, p. 6), tais práticas representam um sério risco, com potencial para “afetar diretamente o cenário político, a segurança nacional e, consequentemente, ameaçar a própria democracia”. De forma ainda mais alarmante, uma pesquisa revelou que 96% dos *deepfakes* na internet eram de natureza pornográfica, sendo 100% deles direcionados a mulheres, o que evidencia a tecnologia como uma nova e cruel ferramenta para a pornografia de vingança e a violência de gênero (Medon, 2021, p. 261).

Diante deste cenário, a análise jurídico-penal se torna totalmente necessária. A criação ou o uso de um *deepfake* não constitui, *a priori*, um crime em si mesmo no ordenamento brasileiro atual.

Contudo, como corretamente apontado em sua pesquisa inicial, essa tecnologia se revela um poderoso instrumento para a prática de crimes já tipificados. Caracteriza-se, portanto, como um meio para a execução de crimes cibernéticos impróprios, como a calúnia, a difamação, a extorsão, o estelionato e, como veremos adiante, diversas formas de violência de gênero e fraudes complexas.

2 A ANÁLISE DOGMÁTICA DA RESPONSABILIZAÇÃO PENAL FRENTE AO USO DE DEEPFAKES

2.1 DA SÁTIRA AO INSTRUMENTO DO CRIME

No contexto da Quarta Revolução Industrial, caracterizada por avanços exponenciais em inteligência artificial e nanotecnologia, surgem inovações que redefinem continuamente as interações humanas. Dentre essas inovações, a tecnologia *deepfake* emergiu como um fenômeno notável.

Em sua origem, suas aplicações eram não apenas lícitas, mas também celebradas em campos como o da indústria cinematográfica e publicitária, onde era utilizada para criar efeitos especiais antes inimagináveis. Um dos casos mais emblemáticos, conforme leciona Medon (2021, p. 269), foi sua utilização no filme *Rogue One: Uma História Star Wars*:

A indústria cinematográfica também já se valeu desta técnica. Um dos casos mais famosos talvez tenha sido o do filme *Rogue One: Uma História Star Wars* (2016), da série homônima, quando se recriaram alguns personagens. O mais peculiar foi, sem dúvidas, o do Comandante Tarkin, interpretado pelo britânico Peter Cushing, pois este ator já havia falecido no ano de 1994. Valendo-se de técnicas computacionais, viabilizou-se a chamada “reconstrução digital” da imagem do já falecido ator, o que desperta questionamentos, como a necessidade de autorização dos herdeiros para a reconstrução de sua imagem. Note-se, contudo, a peculiaridade dessa situação: não se trata de reproduzir novamente imagens captadas em momento pretérito, mas de se criar novas imagens, a partir de capturas anteriores.

Para além do cinema, a tecnologia encontrou um vasto campo na área humorística e na sátira, popularizando-se inicialmente como uma forma de criar paródias e conteúdos cômicos envolvendo, majoritariamente, figuras públicas (Alves, 2024, p. 2). Contudo, como bem pontua a doutrina, mesmo essa utilização para fins de entretenimento já tangenciava os limites da legalidade, pois, a depender do teor da manipulação, a sátira poderia facilmente resvalar para a ofensa à dignidade e à honra das pessoas retratadas nos vídeos (Oliveira, 2024, p. 12).

No entanto, o ponto de inflexão ocorreu quando a tecnologia se democratizou e saiu desses ambientes mais controlados. Sua popularização online, como na plataforma *Reddit*, de onde o próprio termo se originou, marcou o início de sua apropriação para fins inequivocamente ilícitos (Medon, 2021). A primeira onda de uso malicioso, conforme relatam os estudos sobre o tema, manifestou-se na criação de conteúdo pornográfico não consensual, uma prática que evoluiu para se tornar uma nova e cruel ferramenta de “sextorsão” e violência de gênero.

A partir deste momento, a mudança de uma ferramenta de entretenimento para um instrumento criminal se consolidou. O potencial disruptivo dos *deepfakes* foi rapidamente percebido e explorado em outras searas, inclusive na esfera política. Podemos utilizar de exemplo a recente publicação de um “deep fake” de Volodymyr Zelensky, atual presidente da Ucrânia, país que se encontra em guerra com a Rússia, no qual o mesmo aparece anunciando rendição ao exército russo. (Wakefield, 2022).

Dessa forma, o que se observa é que a mesma sofisticação que torna o *deepfake* uma tecnologia revolucionária, é precisamente o que a converte em uma *fake news* qualificada. Ela representa um salto qualitativo na disseminação de desinformação. Por essa razão, a análise que se segue não busca criminalizar a técnica em si, o que seria uma solução ineficiente diante da constante evolução

tecnológica, mas sim compreender como o ordenamento jurídico-penal brasileiro pode e deve responder às condutas ilícitas que se valem desse poderoso instrumento.

2.2 A PLURALIDADE DE BENS JURÍDICOS ATINGIDOS

A análise da responsabilidade criminal no contexto dos *deepfakes* exige do operador do Direito um exercício de subsunção, ou seja, de enquadramento da conduta concreta a um tipo penal previsto em lei.

Uma vez que o ordenamento jurídico brasileiro não possui um crime autônomo de "criação ou disseminação de *deepfake*", a persecução penal se volta para os crimes que utilizam essa tecnologia como um sofisticado *modus operandi*. Nesse diapasão, a ferramenta revela-se assustadoramente versátil, capaz de servir como instrumento para a violação de uma vasta gama de bens jurídicos, que vão desde a honra e a dignidade sexual até o patrimônio e a fé pública (Alves, 2024, p. 1).

O campo mais intuitivo para a aplicação da lei penal é, sem dúvida, o dos crimes contra a honra, previstos nos artigos 138 a 140 do Código Penal, que são divididos entre os crimes de calúnia, injúria e difamação.

O ambiente digital, por sua natureza viral e de alcance em grande escala, já potencializava os danos desses delitos, mas a introdução dos *deepfakes* elevou essa ameaça a um novo patamar de verossimilhança e poder destrutivo. A conduta de criar um vídeo manipulado que atribui falsamente a alguém a prática de um fato definido como crime, como uma agressão ou um ato de corrupção, amolda-se perfeitamente ao tipo penal de calúnia. Para os terceiros que compartilham tal conteúdo, a responsabilização também é possível, conforme prevê o próprio Código Penal, desde que o façam "sabendo ser falsa a informação" (Brasil, 1940).

De modo similar, se a *deepfake* imputar um fato não criminoso, mas ofensivo à reputação da vítima, como um comportamento antiético, por exemplo, a conduta se enquadra na difamação.

Já a injúria, que atinge a honra subjetiva, encontra na *deepfake* um meio cruel para ofender a dignidade e o decoro de uma pessoa, ao colocá-la em situações humilhantes ou proferindo palavras vexatórias. Ciente dessa nova realidade, o Poder Legislativo já debate propostas que visam restringir a manipulação de imagens e aumentar as sanções para crimes contra a honra cometidos em redes sociais, o que demonstra uma tentativa de adequar a legislação ao avanço tecnológico (Alves,

2024).

Contudo, a violação pode atingir esferas ainda mais íntimas e profundas da personalidade. A faceta mais alarmante e, estatisticamente, mais prevalente do uso ilícito de *deepfakes* reside na sua aplicação como ferramenta de violência de gênero, materializada na criação de pornografia não consensual. Uma pesquisa da Deepttrace, citada por Medon (2021), revelou um dado estarrecedor: 96% dos vídeos *deepfake* na internet possuíam conteúdo pornográfico, sendo as mulheres as vítimas em 100% desses casos.

Essa prática, agrava o já repudiado fenômeno do *revenge porn*, encontra possível enquadramento no art. 218-C do Código Penal, que criminaliza a divulgação de cena de sexo ou pornografia sem o consentimento da vítima (Oliveira, 2024, p. 8).

A discussão dogmática que se impõe é se um conteúdo que simula uma cena que jamais ocorreu faticamente, se subsume à elementar cena de sexo. A melhor interpretação, à luz do princípio da máxima proteção do bem jurídico tutelado, é a de que a resposta deve ser afirmativa. A exposição, a humilhação e a violação da intimidade são plenamente configuradas, independentemente da veracidade fática do ato, pois, para o público espectador, a imagem da vítima está inequivocamente associada àquela cena sexualizada, causando danos reais e, muitas vezes, irreparáveis à sua vida (Oliveira, 2024, p. 8).

A versatilidade das *deepfakes* como instrumento delitivo se estende, ainda, à esfera patrimonial. Nos crimes de estelionato (art. 171, Código Penal), a tecnologia se manifesta como o meio fraudulento por excelência, elemento essencial para a configuração do tipo. A capacidade de simular com perfeição a voz de um familiar em apuros para solicitar uma transferência de emergência, ou a imagem e a voz de um alto executivo para autorizar um pagamento fraudulento, cria a armadilha perfeita para induzir a vítima a erro e causar-lhe significativo prejuízo financeiro.

Para além do estelionato, a tecnologia pode ser empregada para a prática de falsidade ideológica (art. 299, Código Penal), notadamente em situações que envolvem a burla de sistemas de segurança baseados em biometria facial, seja para a abertura de contas bancárias ou para a obtenção de vantagens indevidas em nome de terceiros (Brasil, 1940).

Fica claro, portanto, que a ausência de um tipo penal específico para a prática de *deepfake* não resulta em um vácuo legislativo que leve à impunidade. A conduta

de criar e disseminar tais conteúdos, quando dotada de finalidade ilícita, encontra forte repressão no ordenamento jurídico vigente, violando uma pluralidade de bens jurídicos e amoldando-se a diversos crimes já tipificados.

Diante disso, o desafio que se apresenta ao sistema de justiça criminal não é tanto o de criar novas leis, mas o de aplicar com eficácia as existentes, adaptando a interpretação dogmática para abarcar as nuances e a sofisticação dessa nova e perigosa forma de criminalidade.

2.3 A DUPLA FACE DO DESAFIO: A DIMENSÃO DOS DANOS E OS MECANISMOS DE PROTEÇÃO

A análise da subsunção dos atos praticados com *deepfakes* aos tipos penais vigentes revela a ponta visível de um problema muito mais profundo. Para além da classificação dogmática, é imperativo compreender a magnitude dos danos que essa tecnologia pode infligir e, em contrapartida, explorar os mecanismos de defesa disponíveis para a sociedade.

Trata-se de uma dupla face do mesmo desafio: de um lado, a violação de direitos personalíssimos e a instauração de uma crise de confiança, e de outro, a busca por soluções pragmáticas e educacionais naquilo que podemos chamar de era da pós-verdade (Faustino, 2018).

A dimensão dos danos causados por uma *deepfake* maliciosa transcende em muito a esfera patrimonial ou a ofensa reputacional. O impacto mais imediato e, por vezes, mais duradouro, reside nos profundos danos psicológicos infligidos à vítima. A exposição massiva a um conteúdo fabricado, hiper-realista, que viola a intimidade e a imagem de uma pessoa, pode desencadear quadros severos de angústia, ansiedade, depressão e estresse pós-traumático.

Conforme alertam especialistas, a vítima enfrenta um profundo sentimento de humilhação e violação que afeta drasticamente sua vida social, seus relacionamentos e sua carreira profissional. Esse sofrimento psíquico representa uma afronta direta ao princípio da dignidade da pessoa humana, pilar de nosso ordenamento constitucional, que protege o indivíduo em sua integridade moral e psíquica (Alves, 2024).

Essa agressão à esfera íntima se desdobra em danos reputacionais e sociais de difícil reparação. A disseminação de uma *deepfake* pode destruir a imagem pública de uma pessoa, causando prejuízos irreparáveis à sua honra e boa fama. A

capacidade de viralização da internet, somada à dificuldade de desmentir um conteúdo visualmente convincente, cria um cenário de impotência para a vítima, que se vê obrigada a lutar contra uma mentira que se espalha de forma exponencial (Oliveira, 2024).

Essa problemática nos insere em uma verdadeira “crise da verdade”. A eficácia dos *deepfakes* em enganar o público geral ficou evidente em um episódio recente: um vídeo de um canguru de apoio emocional em um voo viralizou, sendo amplamente aceito como real antes de sua origem artificial ser revelada. Se um conteúdo tão incomum é capaz de enganar milhões de pessoas, a capacidade de um *deepfake* malicioso de ser igualmente crível e, portanto, devastador, é inegável (Vilela, 2024).

Portanto, esse fenômeno aniquila a confiança coletiva em registros audiovisuais, com implicações sérias para o jornalismo, para a estabilidade dos processos democráticos e até mesmo para a integridade do sistema de justiça, que pode se ver diante do desafio de distinguir entre provas genuínas e evidências fabricadas.

Diante de um cenário tão complexo, a resposta deve ser multifacetada, combinando a repressão penal com mecanismos de proteção e cautela. A primeira linha de defesa reside no desenvolvimento de soluções tecnológicas e forenses. Pesquisadores têm se dedicado a criar algoritmos capazes de identificar manipulações, em uma espécie de “corrida digital” contra os criadores de *deepfakes*. Um exemplo é o algoritmo *XceptionNet*, desenvolvido pela *Technical University of Munich*, que utiliza o *machine learning* para comparar vídeos e reconhecer padrões de manipulação facial (Bezerra, 2016, p. 126).

Trata-se de um algoritmo de aprendizagem profunda que identifica vídeos cujos rostos foram substituídos por outros. Os pesquisadores coletaram mais de mil vídeos cujos rostos foram substituídos e também os vídeos originais e criaram um banco de dados com mais de meio milhão de imagens de rostos alterados. A partir disto, criaram um banco de dados de rostos manipulados de FaceForensics e utilizaram um modelo de rede neural de aprendizagem profunda para compreender a diferença entre o vídeo real e o vídeo modificado. A partir deste projeto criaram o algoritmo denominado *XceptionNet* que representa uma importante solução para identificar vídeos que sofreram manipulação facial e outras alterações.

Contudo, a proteção não pode depender apenas de especialistas. É crucial capacitar o cidadão comum a identificar possíveis fraudes. A ciência forense e a segurança digital apontam para alguns sinais práticos que podem denunciar uma manipulação como, anomalias faciais e oculares, sincronia labial e áudio, por exemplo

(Oliveira, 2024, p. 12).

Além da análise técnica individual, a proteção se fortalece com respostas institucionais e, principalmente, educacionais. A atuação de órgãos como o Comitê Gestor da Internet no Brasil (CGI.br), que publica materiais como a Cartilha de Segurança para Internet, é fundamental para orientar os usuários sobre como se proteger de ameaças online. No âmbito familiar, o diálogo aberto sobre os perigos da internet e o uso de ferramentas de controle parental são essenciais para proteger crianças e adolescentes (CGI, 2012, p. 3).

Em uma última análise, a defesa mais robusta e sustentável contra a desinformação semeada pelos *deepfakes* é a educação digital. A promoção de competências em "educação para a mídia" (*media literacy*), conforme já proposto pela Comissão Europeia, é o caminho para auxiliar os usuários a navegarem em um mundo com grande quantidade de informações. Fomentar uma cultura de ceticismo saudável, de verificação de fontes e de resistência ao compartilhamento impulsivo é a principal barreira na luta pela preservação da verdade e pela proteção dos direitos da personalidade na era digital (Almeida, 2020).

3 A QUALIFICADORA COMO SOLUÇÃO: A PUNIÇÃO DE CRIMES COM *DEEP FAKES* NO ORDENAMENTO BRASILEIRO

A jornada que percorremos até aqui, partindo da conceituação do fenômeno *deepfake* e passando pela subsunção das condutas aos tipos penais existentes, nos conduz, inevitavelmente, ao cerne da problemática jurídica: a adequação e a suficiência da resposta legislativa brasileira.

O avanço tecnológico impõe ao Direito Penal um desafio constante, forçando-o a se equilibrar sobre uma linha tênue. De um lado, encontra-se o dever estatal de garantir a segurança dos cidadãos, materializado no princípio da proibição da proteção deficiente, que veda a inércia do legislador diante de novas e graves ameaças aos direitos fundamentais.

De outro, ergue-se como pilar do Estado Democrático de Direito o princípio da legalidade, consagrado no artigo 1º do Código Penal, que proíbe a punição de qualquer ato não previsto expressamente em lei (Brasil, 1940). É nesse campo de tensão que a discussão sobre a necessidade de uma nova lei para criminalizar os *deepfakes* deve ser travada.

A ideia de criar um tipo penal autônomo, embora possa parecer uma resposta intuitiva, revela-se, sob um olhar mais aprofundado, uma solução juridicamente frágil e ineficaz, visto que, o principal obstáculo reside na própria natureza do princípio da legalidade, que se desdobra em garantias como a da reserva legal, exigindo que apenas a lei em sentido estrito crie crimes, e, crucialmente, a da taxatividade, que demanda clareza e precisão na descrição da conduta criminosa.

O ritmo da inovação tecnológica é exponencialmente mais rápido que o do processo legislativo, ou seja, criminalizar a técnica específica do *deepfake* hoje significaria criar uma norma destinada à obsolescência, pois amanhã novas tecnologias de manipulação audiovisual, talvez com outros nomes e métodos, certamente surgirão, deixando a lei um passo atrás e criando novas lacunas (Alves et al., 2024, p. 17). A solução mais perene, portanto, não é focar na ferramenta, mas sim na conduta lesiva que se pratica com ela, conforme aduz a doutrina ao afirmar que a resposta mais eficiente seria criminalizar as condutas praticadas através da tecnologia, e não a tecnologia em si (Lima Filho, 2021, *apud* Alves et al., 2024, p. 17).

Ademais, conforme demonstrado, as condutas maliciosas já encontram, em sua essência, enquadramento em crimes existentes. A ofensa à honra, à violação da dignidade sexual e o estelionato são os resultados danosos que o Direito Penal já se propõe a coibir, portanto, o problema não é a atipicidade absoluta da conduta-fim, mas o reconhecimento de que o *modus operandi* do uso de uma simulação hiper-realista, agrava a conduta, potencializando o dano, dificultando a defesa da vítima e aumentando a sensação de impunidade do agressor, que se beneficia do caos informacional e da dificuldade de rastreamento (Oliveira; Ávila, 2024, p. 12).

Por isso que a resposta legislativa mais técnica, proporcional e eficiente consiste na criação de uma qualificadora ou de uma causa de aumento de pena para os crimes que se valem dessa tecnologia.

Esta abordagem possui múltiplas vantagens, primeiramente, ela respeita a estrutura dogmática do Código Penal, pois reconhece que a base do ilícito permanece a mesma, mas que o meio empregado o torna mais reprovável, justificando uma sanção mais severa. Em segundo lugar, ela oferece uma solução mais duradoura ao prever um aumento de pena para crimes cometidos com o uso de *deepfakes* ou expressão similar, a lei consegue abarcar não apenas os *deepfakes* de hoje, mas também as tecnologias análogas que surgirão no futuro, evitando a rápida defasagem

da norma. O ordenamento pátrio já utiliza essa técnica com sucesso, como no caso do artigo 122, §4º, do Código Penal, que majora a pena quando o crime de induzimento ao suicídio ou à automutilação é realizado por meio da rede de computadores ou rede social (Brasil, 1940).

A omissão do Estado em adaptar sua resposta punitiva a essa nova realidade configura uma proteção deficiente dos direitos fundamentais, violando um dever constitucional. A aplicação correta e proporcional da sanção penal é mais que um direito, é um poder-dever do Estado para garantir a harmonia e a segurança jurídica, como brilhantemente exposto por Da Costa:

Miguel Reale Júnior aponta que a aplicação correta do Direito Penal e de suas sanções constituem mais que um direito, um poder do Estado, que, almejando assegurar a harmonia social, não pode deixar de atuar e deixar ao talante dos particulares sua efetividade. Se assim agisse teríamos uma *capitis diminutio*, com a fragilização da soberania e o surgimento de uma profunda insegurança jurídica para a sociedade, de sorte que a eficácia da norma estaria limitada ao interesse da vítima ou de sua família, gerando inclusive ao infrator uma insegurança jurídica e ao Estado uma limitação da aplicabilidade da lei. (Da Costa, 2011, p. 33-34)

Essa citação reforça que a inércia não é uma opção. O caminho legislativo já começa a ser trilhado nessa direção, como se observa no Projeto de Lei nº 146/2024, que propõe o aumento da pena para crimes contra a honra e qualifica o crime de falsa identidade quando a tecnologia de inteligência artificial é empregada (Senado Federal, 2024).

Esta é a via que se mostra mais promissora, pois equaciona a necessidade de uma punição mais rigorosa com o respeito aos princípios basilares do Direito Penal.

Em suma, conclui-se que a jornada para a responsabilização penal eficaz de criadores e propagadores de *deepfakes* não requer a invenção de um novo tipo penal, mas sim o aprimoramento inteligente da legislação existente. Ao inserir qualificadoras ou causas de aumento de pena nos crimes que podem ser instrumentalizados por essa tecnologia, o legislador estará preservando a coerência do sistema, evitando a armadilha da obsolescência tecnológica e, oferecendo uma proteção mais robusta e proporcional à dignidade, à honra e à imagem da pessoa humana na complexa era digital.

CONSIDERAÇÕES FINAIS

O presente artigo, retrata um dos desafios mais complexos impostos ao Direito Penal contemporâneo: a responsabilização criminal pela criação e disseminação de *deepfakes*.

A ascensão desta tecnologia, permite a manipulação hiper-realista de conteúdos audiovisuais por meio de inteligência artificial, e representa uma profunda ruptura, não apenas tecnológica, mas também social e jurídica. Ao longo deste trabalho, foi demonstrado como uma ferramenta inicialmente associada à indústria do entretenimento e à sátira transformou-se em um poderoso instrumento para a prática de ilícitos, violando uma grande variedade de bens jurídicos importantes à pessoa humana, como a honra, a imagem, a privacidade e a dignidade sexual.

A pesquisa partiu da análise da inserção das *deepfakes* no contexto mais amplo dos crimes cibernéticos, classificando-os como um meio para a prática de crimes impróprios, ou seja, aqueles em que a tecnologia serve como um *modus operandi* para delitos já existentes no ordenamento jurídico.

Verificou-se que condutas como a imputação falsa de crimes, a ofensa à reputação, as fraudes financeiras e, de forma especialmente alarmante, a criação de pornografia não consensual, encontram, em tese, subsunção em tipos penais como a calúnia, a difamação, o estelionato e o crime previsto no artigo 218-C do Código Penal.

Contudo, a mera possibilidade de enquadramento legal revelou-se insuficiente para esgotar a problemática, por isso, a investigação adentrou o debate dogmático, ponderando a tensão entre, o princípio da proibição da proteção deficiente, que impõe ao Estado o dever de tutelar de forma eficaz os direitos fundamentais, e, de outro, o princípio da legalidade estrita, que veda a punição de condutas não expressamente previstas em lei. A questão central que norteou o capítulo final foi, portanto, definir qual a resposta legislativa mais adequada para o fenômeno.

Diante do exposto, este trabalho conclui que a criação de um tipo penal autônomo para a prática de *deepfake* não seria a solução mais técnica, eficiente e duradoura. Tal medida, embora possa parecer uma resposta enérgica, incorreria no risco da rápida obsolescência, uma vez que a velocidade da inovação tecnológica supera em muito o ritmo do processo legislativo, ou seja, criminalizar a ferramenta, e não a conduta lesiva, seria uma estratégia ineficaz.

A tese defendida e consolidada ao final desta pesquisa é a de que o caminho mais coerente e mais eficaz do ponto de vista da política criminal é o aprimoramento

da legislação existente por meio da criação de qualificadoras ou causas de aumento de pena. O uso de inteligência artificial para a manipulação de imagem e voz deve ser tratado como uma circunstância que agrava a reprovabilidade da conduta, justificando uma sanção mais severa.

Essa proposta encontra respaldo em iniciativas legislativas, como o Projeto de Lei nº 146/2024, e se alinha à técnica já utilizada pelo legislador em outras situações, como nos crimes contra a dignidade sexual praticados pela Internet, onde a inserção de uma majorante preserva a coerência do sistema, evita a indesejada inflação penal e oferece uma proteção mais robusta e adaptável às futuras evoluções tecnológicas.

Por fim, é imperativo reconhecer que a resposta ao desafio dos *deepfakes* não se esgota na esfera penal, a repressão é fundamental, mas a prevenção, por meio da educação digital e do fomento da educação para a mídia (*media literacy*), é igualmente crucial para construir uma sociedade mais resiliente à desinformação. O caminho para a proteção efetiva da dignidade da pessoa humana na complexa era digital passa, necessariamente, pela adaptação inteligente da lei, aliada a um esforço coletivo de conscientização e capacitação crítica.

REFERÊNCIAS

ALMEIDA, Fernanda Campo. *Deepfake*: tecnologia permite colocar rosto e voz em outro corpo. **Veja São Paulo**, jul. 2020. Disponível em: <https://vejasp.abril.com.br/cultura-lazer/deepfake-tecnologia-permite-copiar-o-rosto-expressao-e-a-voz/>. Acesso em: 28 ago. 2025.

ALVES, Bruno Moraes *et al.* Análise da responsabilização criminal dos criadores e propagadores de “*deep fakes*” no ordenamento jurídico brasileiro. **Communication and Culture: Multidisciplinary Perspectives**, 2024. Disponível em: <https://doi.org/10.56238/sevened2024.014-011>. Acesso em: 26 ago. 2025.

BEZERRA, Clayton da Silva; AGNOLETTI, Giovani Celso (Org.). **Combate às Fake News**. 1. ed. São Paulo: Editora Posteridade, 2019.

BRASIL. Câmara dos Deputados. **Relatório Final da Comissão Parlamentar de Inquérito (CPI) dos Crimes Cibernéticos**. Brasília, DF: Câmara dos Deputados, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1455189. Acesso em: 18 ago. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. Disponível em:

https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 ago. 2025.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e revoga o art. 65 da Lei nº 7.716, de 5 de janeiro de 1989. **Diário Oficial da União**, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 18 ago. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Diário Oficial da União**, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 ago. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 ago. 2025.

BRASIL. Senado Federal. Agência Senado. Projetos buscam restringir manipulação de imagens com inteligência artificial. **Agência Senado Notícias**, 7 fev. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/02/07/projetos-buscam-restringir-manipulacao-de-imagens-com-inteligencia-artificial>. Acesso em: 28 ago. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 28 ago. 2025.

DA COSTA, Fernando José. **Locus delicti nos crimes informáticos**. 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php>. Acesso em: 22 set. 2025.

EQUIPE PROJURIS. **Lei Carolina Dieckmann**: o que é e o que diz a Lei 12.737/12. Projuris, 15 mar. 2023. Disponível em: <https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/>. Acesso em: 18 ago. 2025.

EQUIPE PROJURIS. **Marco Civil da Internet**: o que é, e quais seus principais pontos. Projuris, 15 mar. 2024. Disponível em: <https://www.projuris.com.br/blog/marco-civil-da-internet/>. Acesso em: 18 ago. 2025.

FAUSTINO, André. **Fake news e a liberdade de expressão nas redes sociais na sociedade da informação**. 2018. 140 f. Dissertação (Mestrado em Direito da Sociedade da Informação) – Faculdades Metropolitanas Unidas, São Paulo, 2018.

Disponível em: <http://arquivo.fmu.br/prodisc/mestradodir/af.pdf>. Acesso em: 18 ago. 2025.

GRAN FACULDADE. **Crimes cibernéticos: o que são, leis e casos no Brasil**. Gran Faculdade, 13 mar. 2024. Disponível em: <https://faculdade.grancursosonline.com.br/blog/crimes-ciberneticos/#conceito>. Acesso em: 18 ago. 2025.

GZH. **Após atingir pico de óbitos, Brasil tem queda de 90% na média diária de mortes por covid-19**. GZH Saúde, 28 out. 2021. Disponível em: <https://gauchazh.clicrbs.com.br/saude/noticia/2021/10/apos-atingir-pico-de-obitos-brasil-tem-queda-de-90-na-media-diaria-de-mortes-por-covid-19-ckuxys2ts0007017fzwxl3u0e.html>. Acesso em: 18 ago. 2025.

INTERNET MATTERS. **O que é uma deepfake?** Internet Matters, 2023. Disponível em: <https://www.internetmatters.org/pt/resources/what-is-a-deepfake/>. Acesso em: 18 ago. 2025.

KASPERSKY. **Como se proteger de deepfakes**. Kaspersky Resource Center, [s. d.]. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake>. Acesso em: 28 ago. 2025.

LACERDA, Anna Carolina Alves Moreira de; SILVA, Amanda Pedroso. Cibercrime: evolução do crime e a banalização dos crimes virtuais. In: HORITA, Fernando Henrique da Silva; MORAIS, Fausto Santos de; OLIVEIRA, Camila Martins de (Org.). **Direito Penal e Cybercrimes**. 1. ed. Belo Horizonte: Skema Business School, 2021. v. 1, p. 12-19.

LIMA FILHO, Paulo Roberto Aguiar de. O Direito Penal na Quarta Revolução Industrial. *Delictae: Revista De Estudos Interdisciplinares Sobre O Delito*, v. 6, n. 10, p. 215-304, 2021. Disponível em: <https://doi.org/10.24861/25265180.v6i10.150>. Acesso em: 18 ago. 2025.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. **RIOS Eletrônica (FASETE)**, v. 12, n. 18, p. 166-180, 2018. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf. Acesso em: 18 ago. 2025.

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: <https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/438/447>. Acesso em: 18 ago. 2025.

MIGALHAS. **Sancionadas leis que tratam de crimes cibernéticos**. Migalhas, 2 dez. 2012. Disponível em: <https://www.migalhas.com.br/quentes/168701/sancionadas-leis-que-tratam-de-crimes-ciberneticos>. Acesso em: 18 ago. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **O que é a LGPD**. MPF, [s. d.]. Disponível em: <https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd>. Acesso em: 18 ago. 2025.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha de. Deep fake,

direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 19, e85239, p. 1-19, 2024. Disponível em: <https://doi.org/10.5902/1981369485239>. Acesso em: 26 ago. 2025.

PEREIRA, Allan Andrade. A evolução do crime de deepfake e o direito penal brasileiro. **Revista Multidisciplinar Científica**, v. 3, n. 7, p. 1-18, 2023. Disponível em: <https://sevenpublicacoes.com.br/editora/article/download/4883/8785/19489>. Acesso em: 18 ago. 2025.

ROCHA, Lucas. Deepfakes causam danos duradouros às crianças; veja como protegê-las. **CNN Brasil**, 22 fev. 2024. Disponível em: <https://www.cnnbrasil.com.br/saude/deepfakes-causam-danos-duradouros-as-criancas-veja-como-protege-las/>. Acesso em: 28 ago. 2025.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

SIQUEIRA, Paulo Alexandre Rodrigues de. O 'Deep Fake' e a Legislação Brasileira: utilização de instrumentos legais para a proteção à imagem. **Conteúdo Jurídico**, Brasília, DF, 29 set. 2021. Disponível em: <https://conteudojuridico.com.br/consulta/artigo/53256/o-deep-fake-e-a-legislao-brasileira-utilizao-deinstrumentos-legais-para-a-proteo-imagem>. Acesso em: 28 ago. 2025.

VILELA, Manuela. Deepfake, golpes e desinformação: os efeitos colaterais dos vídeos de IA ultrarrealistas. **Forbes Brasil**, 27 jun. 2024. Disponível em: <https://forbes.com.br/escolhas-do-editor/2025/06/deepfake-golpes-e-desinformacao-os-efeitos-colaterais-dos-videos-de-ia-ultrarrealistas/>. Acesso em: 28 ago. 2025.

A R T I G O 06

DIREITO À EDUCAÇÃO E OS OBSTÁCULOS À INCLUSÃO DE ALUNOS COM DEFICIÊNCIA NO SISTEMA REGULAR DE ENSINO: ANÁLISE DA EFICÁCIA DA LEGISLAÇÃO BRASILEIRA

Melissa Matos Araújo
Williane Tibúrcio Facundes