

Recebido em: 10/04/2026

Aceito em: 20/09/2026

DOI: 10.25110/rcjs.v29i1.2026-12740



IMPACTOS DAS TÉCNICAS DE *DEEPPFAKE* NO DIREITO BRASILEIRO E A PROTEÇÃO DE CRIANÇAS E ADOLESCENTES

IMPACTS OF *DEEPPFAKE* TECHNIQUES IN BRAZILIAN LAW AND THE PROTECTION OF CHILDREN AND ADOLESCENTS

Daniele Deidio

Bacharel em Direito pela Pontifícia
Universidade Católica do Paraná.

daniele.deidio@pucpr.edu.br

<https://orcid.org/0009-0005-6083-4570>

*Cinthia Obladen de
Almendra Freitas*

Doutora em Informática pela Pontifícia
Universidade Católica do Paraná, Brasil.
Professora Titular da Escola de Direito e
do Programa de Pós-Graduação em
Direito da mesma instituição.

cinthia.freitas@pucpr.br

<https://orcid.org/0000-0002-7015-094X>

RESUMO: A presente pesquisa explora os limites do ordenamento jurídico brasileiro quanto ao aliciamento de crianças e adolescentes por meio da aplicação de técnicas de *deepfake*. Com os avanços tecnológicos e ampla disponibilidade de ferramentas de manipulação de imagens e vídeos, somada à ingenuidade das crianças e adolescentes, torna-se essencial analisar como tais técnicas podem ser utilizadas por criminosos para aliciar suas vítimas. Pelo método dedutivo e procedimentos bibliográficos, analisou-se como essa tecnologia é utilizada por criminosos no ambiente digital e suas consequências jurídicas. O objetivo geral consiste em compreender os limites no direito brasileiro para coibir ou mitigar os riscos de aliciamento de crianças e adolescentes diante da aplicação de técnicas de *deepfake*. A pesquisa busca responder o que é *deepfake*, como é aplicado para aliciar crianças e adolescentes e quais as consequências jurídicas, especialmente penais, no âmbito brasileiro. Compreendeu-se que aliciadores podem utilizar técnicas de *deepfake* para conhecer, se aproximar, facilitar o convencimento e abusar das vítimas. Constatou-se que, embora existam normas de proteção à imagem e personalidade, não há regulamentação específica sobre *deepfake*, especialmente no contexto de aliciamento. Conclui-se que, para garantir que o ordenamento jurídico brasileiro seja capaz de responder adequadamente às novas formas de atuação da criminalidade, se faz necessária a criação e aprovação de leis específicas que abranjam o uso de técnicas de *deepfake* contra crianças e adolescentes.

PALAVRAS-CHAVE: Aliciamento; Crianças e adolescentes; *Deepfake*; Direito e Tecnologia; Direito Penal.

ABSTRACT: The present research explores the limits of the Brazilian legal system regarding the grooming of children and adolescents through the application of deepfake techniques. With technological advances and the wide availability of image and video manipulation tools, combined with the naivety of children and adolescents, it becomes essential to analyze how such tools may be used by criminals to groom their victims. Through the deductive method and bibliographic procedures, it was analyzed how this technology is used by criminals in the digital environment and its legal consequences. The general objective is to understand the limits within Brazilian law to prevent or mitigate the risks of grooming children and adolescents considering the application of deepfake techniques. The research seeks to answer what deepfake is, how it is applied to groom children and adolescents, and what the legal consequences are, especially criminal ones, within the Brazilian context. It was understood that groomers may use deepfake techniques to meet, approach, facilitate persuasion, and abuse victims. It was found that, although there are rules protecting image and personality rights, there is no specific regulation regarding deepfake, especially in the context of grooming. It is concluded that, to ensure that the Brazilian legal system is capable of adequately responding to new forms of criminal activity, it is necessary to create and approve specific laws that encompass the use of deepfake techniques against children and adolescents.

KEYWORDS: Grooming; Children and adolescents; Deepfake; Law and technology; Criminal law.

Como citar: DEIDIO, Daniele; FREITAS, Cinthia Obladen de Almendra. Impactos das técnicas de *deepfake* no direito brasileiro e a proteção de crianças e adolescentes. *Revista de Ciências Jurídicas e Sociais da UNIPAR*, Umuarama, v. 29, n. 1, p. 223-247, 2026.

INTRODUÇÃO

Reconhecer pessoas é uma atividade humana. O ser humano aprende a reconhecer uma pessoa a partir do momento que a conhece. O modelo mental de reconhecimento de humanos é uma tarefa complexa e exige não só o aprendizado, mas a capacidade de atribuir alterações ou variações ao longo do tempo. Tem-se a capacidade de reconhecer alguém que já envelheceu ou está de óculos ou chapéu ou barba.

O reconhecimento facial é uma dessas atividades humanas que são passíveis de reprodução por sistemas de Inteligência Artificial com base em técnicas de reconhecimento de imagens, as quais fazem parte da área de Visão, que por sua vez é um dos ramos da Inteligência Artificial (IA) (Kumar, 2018).

Mas é possível simular computacionalmente um rosto humano? Pode uma pessoa se passar por outra pessoa, de modo a enganar ou ludibriar alguém? Ambas as respostas são sim. A temática do uso de técnicas de *deepfake* e aliciamento de crianças e adolescentes (*grooming*) foi tema da novela “Travessia” (Souza, Helder, 2023). No enredo da novela, um aliciador se utilizava de técnicas de *deepfake* para se passar por uma modelo e influenciadora digital e aliciar adolescentes. O aliciador fazia uso de um aplicativo gerador de *deepfake* e assim modificava áudio e vídeo em tempo real para ludibriar a vítima, se aproximar e conseguir fotos íntimas de uma personagem adolescente. Fora da ficção, infelizmente, esse cenário pode ser replicado de maneira relativamente simples por meio de aplicativos que disponibilizam técnicas de *deepfake* gratuitamente para qualquer usuário.

Como ambiente digital, a Internet apresenta algumas preocupações de segurança cibernética, visto os diferentes tipos de problemas que a sociedade mundial enfrenta atualmente, tais como: invasão de privacidade, descumprimentos de contratos celebrados pela Internet, disseminação de e-mails caluniosos ou difamatórios, pornografia infantil, assédio sexual, *cyberbullying*, compartilhamento ilícito de software, música e filmes, entre outros; ou seja, os denominados: crimes cibernéticos.

Ao mesmo tempo em que a Internet simplifica as operações realizadas no meio digital, insere um fator restritivo e aponta para um universo de estudos sobre os aspectos relacionados à segurança, confiabilidade e autenticidade de

dados. Sem esquecer, ainda, da legalidade dessas operações frente a fatos duvidosos e questionados por qualquer uma das partes envolvidas.

Quando o assunto envolve criança e adolescente, a preocupação é ainda maior, visto que estes têm aguçado o espírito por descoberta e ao mesmo tempo pouca maturidade e baixa precaução com o uso da tecnologia, avaliando de forma simplificada as consequências de suas ações. É fato que no mundo digital há uma espécie de competição entre alguns adolescentes pela disponibilização na Internet de vídeos cada vez mais comprometedores do ponto de vista de conduta sexual para a idade, considerando-se as diversas notícias veiculadas na mídia.

Além disto, a Internet possibilita às crianças e aos adolescentes um mundo sem fronteiras e como consequência, dependendo do ponto de vista e maturidade, sem leis/limites ou controle, o que os transporta para um lugar distante da realidade ou do mundo físico. O problema é que neste contexto, as crianças e adolescentes perdem a noção do alcance da Internet e postam em *blogs*, *fotologs*, redes sociais ou veiculam por aplicativos de mensagens instantâneas ou multiplataforma, entre outros; informações (textos, imagens e vídeos) e opiniões que no mundo físico geralmente comentariam numa roda de amigos ou numa festa com um grupo restrito. Porém, quando este conteúdo vai para a Internet perde-se o controle sobre sua disseminação.

A ingenuidade torna as crianças e os adolescentes alvos fáceis para os mais variados tipos de assédio, especialmente o aliciamento (do inglês, *grooming* ou *enticement*), que pode ser praticado por terceiros que obtiveram dados pessoais ou não. Terceiros se valem da ingenuidade, do espírito de descoberta/liberdade, autossuperação e competição entre crianças/adolescentes para oferecer oportunidades ou experiências únicas com a intenção de tirar proveito da situação.

Considerando o exposto e os resultados obtidos, desde 2011, em projeto de pesquisa intitulado “Detecção de Aliciamento de Crianças e Adolescentes na Internet” (Santin *et al.*, 2012), tem-se que o problema de pesquisa ainda é atual e urgente, visto que o projeto está focado na problemática do aliciamento de crianças e adolescentes que utilizam meios para conversação (salas de bate-papo ou redes sociais), via celulares ou computadores, para conversar com outros amigos (que pensam ser amigos) e deste modo compartilhar seus

hábitos, gostos, angústias e alegrias com terceiros. Atualmente, os estudos integram o projeto aprovado na Chamada Universal 10/2023 do CNPq.

Assim, sabe-se que indivíduos mal-intencionados conhecem esta tendência comportamental das crianças e adolescentes e usam as salas de bate-papo e as redes sociais para o aliciamento com o intuito de praticar desde a coleta de imagens e vídeos de nudez até o abuso sexual, entendendo-se por abuso sexual, “o aliciamento, indução, assédio ou coação de criança ou adolescente com a finalidade de praticar ato libidinoso” (Rashid, 2008).

Tal problema é relevante ao Direito Criminal e à Criminologia, mas envolve o estudo de técnicas computacionais para o entendimento dos procedimentos associados às técnicas de *deepfake* com o intuito de ludibriar crianças e adolescentes. Os estudos têm por base a Teoria da Comunicação Ludibriante (*Luring Communication Theory*) (Freitas; Barbosa; Santin, 2016) por meio da qual pode-se classificar os estágios de uma conversação, a partir do ponto de vista do aliciador, de modo a estabelecer o risco ao qual as crianças e adolescentes estão expostas quando estabelecem uma conversa com um desconhecido em meio digital.

A Teoria da Comunicação Ludibriante (*Luring Communication Theory*), proposta por Olson *et al.* (2007), também abordada por Santin (2013) e Santin *et al.* (2012), apresenta os estágios desenvolvidos pelos aliciadores para atrair suas vítimas, englobando as seguintes etapas: ganho de acesso, verdade enganosa e a iniciação e manutenção do relacionamento sexual. Inicialmente, o agressor busca conhecer, se aproximar e construir uma relação com a vítima, trocando informações acerca das características pessoais e marcando o primeiro encontro. Na segunda etapa, que dura até o contato e abuso sexual, os agressores visam preparar a vítima por meio de estratégias de convencimento para ganhar sua confiança e assim, alcançar seu objetivo final. Depois disso, os aliciadores iniciam propriamente o abuso sexual e, normalmente, por meio de coação, ameaças ou simplesmente convencimento da vítima, mantêm o abuso sexual.

Diante desse cenário, a presente pesquisa teve como objetivo geral o estudo dos limites no Direito brasileiro para coibir ou mitigar os riscos de aliciamento de crianças e adolescentes diante da aplicação de técnicas de *deepfake*. A pesquisa buscou responder aos seguintes questionamentos, ou

objetivos específicos: (i) O que é *deepfake* e como é aplicado para ludibriar crianças e adolescentes nas redes sociais? (ii) O aparato normativo brasileiro, levando em conta a proteção de crianças e adolescentes, impede ou não a aplicação de *deepfake* com o intuito de aliciamento na Internet? (iii) Além do aparato normativo brasileiro que outros setores podem auxiliar na prevenção do aliciamento de crianças e adolescentes na Internet? A fim de facilitar a compreensão acerca dos limites normativos existentes na legislação brasileira, tornou-se fundamental compreender as leis vigentes no país acerca da proteção das crianças e adolescentes e ao uso de técnicas de *deepfake*. Foi abordada a origem e abrangência das principais normativas brasileiras vigentes relacionadas com a temática e, posteriormente, identificadas suas lacunas quanto às técnicas de *deepfake*.

Para tanto, utilizando-se do método dedutivo e procedimentos bibliográficos, realizou-se a leitura e análise de obras bibliográficas e artigos científicos sobre os temas: aliciamento, IA, *deepfake* e reconhecimento de imagens; para então contextualizar a possibilidade de utilização de técnicas de *deepfake* para aliciar crianças/adolescentes e, ainda, como agem os aliciadores, especialmente no ambiente digital.

Para a coleta e seleção dos conteúdos utilizados como base na pesquisa foi estabelecido um protocolo prévio. Foram definidas as palavras-chaves a serem utilizadas nas buscas pelos materiais, tais como: “inteligência artificial”, “aliciamento” e “*deepfake*”. Em seguida, foram selecionadas bases de dados confiáveis, como as ferramentas do Google Acadêmico, Scielo e repositórios científicos CAPES. Foram selecionados os artigos que mais se adequaram ao objetivo da pesquisa, levando em consideração a relevância e a atualidade dos conteúdos.

1. COMPREENDENDO A APLICAÇÃO DE TÉCNICAS DE DEEPPFAKE NO ALICIAMENTO DE CRIANÇAS E ADOLESCENTES NA INTERNET

A IA é um ramo da Ciência da Computação que se originou nos meados da década de 50 e vem sendo bastante pesquisado e aprimorado nos últimos

anos. Essa área do conhecimento pode ser definida de diversas maneiras, definições essas, que de acordo com Norvig e Russell (2013, p. 25) se enquadram em 04 (quatro) linhas de pensamento:

a) Sistemas que pensam como seres humanos: “O novo e interessante esforço para fazer os computadores pensarem... máquinas com mentes, no sentido total e literal” (Haugeland, 1985);

b) Sistemas que atuam como seres humanos: “A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas” (Kurzweil, 1990);

c) Sistemas que pensam racionalmente: “O estudo das computações que tornam possível perceber, raciocinar e agir” (Winston, 1992);

d) Sistemas que atuam racionalmente: “A Inteligência Computacional é o estudo do projeto de agentes inteligentes” (Poole; Goebel; Mackworth, 1998).

Na contemporaneidade, essas linhas de raciocínio são exploradas para estudar e definir a IA. Em resumo, as definições dispostas nos itens ‘a’ e ‘c’ se referem a processos de pensamento e raciocínio, enquanto as dispostas nos itens ‘b’ e ‘d’ se relacionam ao comportamento. Ademais, quanto à maneira com que se pode medir o sucesso de um sistema baseado em técnicas de IA, os itens ‘a’ e ‘b’ aferem a fidelidade ao desempenho humano e os itens ‘c’ e ‘d’ comparam o sistema baseado em técnicas de IA ao conceito ideal de inteligência, denominado racionalidade (Norvig; Russell, 2013).

Um sistema inteligente é capaz de reproduzir capacidades humanas, tais como lógica de entendimento, conhecimento, aprendizagem, racionalidade, planejamento, criatividade, pensamento crítico e solução de problemas (Gottfredson, 1997). Já um sistema considerado racional é aquele que “faz tudo certo”. Com isso, à medida em que o sistema adquire experiência ao reproduzir as funções humanas por meio da implementação de métodos e técnicas, os sistemas de IA vão sendo preparados para se moldar a cada situação e adotar a melhor ação possível (Norvig; Russell, 2013). Assim, pode-se entender que o termo IA é utilizado, normalmente, para fazer referência aos algoritmos implementados em máquinas que realizam funções cognitivas humanas associadas com a própria mente e estabelecem um procedimento de treinamento (*training*) baseado em dados que representam situações, fato e

elementos já ocorridos para, então, predizer ou apontar decisões de futuro. Este procedimento é tecnicamente denominado de aprendizagem.

A aplicação de sistemas de IA em foco neste estudo é o reconhecimento de imagens que inclui métodos e técnicas que possibilitam capturar, armazenar e processar imagens digitais (Stair *et al.*, 2021). O reconhecimento de imagens digitais integra o ramo de Visão Computacional (*Computer Vision*) e está associado também ao ramo de Aprendizagem de Máquina (*Machine Learning*) (Freitas, 2025, p. 71-97) (Smola; Vishwanathan, 2008, p. 3-6).

A visão computacional busca replicar o comportamento humano realizado a partir do sentido da visão, com base na extração de dados e informações de imagens digitais e ou vídeos obtidos a partir de diferentes tipos de sensores e dispositivos. Os sistemas de visão computacional são preparados para reconhecer, distinguir, manipular e processar as informações de um cenário (estático – imagem ou dinâmico – vídeo) considerando padrões no ambiente, objetos ou características biométricas de seres humanos que estejam em tais cenários. Um sistema de visão computacional, de modo geral, recebe dados para serem processados de modo a tomar decisões a partir de resultados obtidos considerando a finalidade do sistema (Ballard; Brown, 1982) (Shah, 2002, p. 101).

A aplicação de técnicas de *deepfake* vai além do reconhecimento de padrões em imagens digitais, sendo possível substituir (adulterar) a face de uma pessoa por outra em uma imagem digital ou vídeo. Para isso, Freitas (2025, p. 76-77) explica que são utilizados algoritmos denominados *Deep Learning*, os quais implementam estruturas semelhantes à rede neural do cérebro humano, de modo que os dados são submetidos a inúmeras camadas (*layers*) de processamento não linear, simulando a maneira de acionar os neurônios (Skansi, 2018). Portanto, *Deep Learning* especifica uma classe de redes neurais artificiais, que por sua vez são uma classe especial de algoritmos de *Machine Learning*, aplicáveis ao processamento de linguagem natural, visão computacional e robótica. Quando o objetivo é gerar faces humanas ou substituir faces humanas em imagens e vídeos, tais algoritmos são aplicados com o intuito de extrair características faciais de uma pessoa em diversos ângulos e/ou movimentos, para posteriormente usar tais informações na criação de imagens/vídeos adulterados.

Os primeiros relatos de sua utilização ocorreram em 2017, inicialmente para geração de conteúdos adultos, sendo posteriormente aprimorada com o uso do chamado *FakeApp* (Moraes, 2020). O método baseia-se no treinamento paralelo de *autoencoders*, compostos por uma rede codificadora e outra decodificadora. O processo inicia-se com a compilação de imagens alinhadas da face de duas pessoas distintas, “A” e “B”. O algoritmo é treinado para reconstruir as faces de “A” a partir de suas próprias imagens, e o mesmo ocorre com “B”. Para gerar a imagem adulterada, compartilha-se a parte de codificação, mantendo separadas as respectivas decodificações. Assim, uma imagem com a face de “A” pode ser codificada pela estrutura compartilhada e decodificada pela decodificadora de “B”. Com isso, é possível gerar um codificador para as informações contextuais do rosto (iluminação, posição e expressão) e um decodificador para as informações morfológicas do rosto (formas e detalhes). A última etapa consiste em utilizar a imagem ou vídeo alvo, extrair e alinhar a face alvo de cada quadro, usar o *autoencoder* modificado para gerar outra face com a mesma iluminação e expressão, por exemplo, e então mesclá-lo de volta à imagem ou vídeo original, gerando-se assim o conteúdo adulterado (Afchar *et al.*, 2018).

À medida em que essa técnica foi sendo aperfeiçoada, seus resultados se tornaram extremamente convincentes e está ficando cada vez mais difícil diferenciar a imagem/vídeo real daquela criada artificialmente. Apesar de se tratar de um processo tecnicamente complexo, atualmente, existem diversos aplicativos que disponibilizam técnicas de *deepfake* para qualquer usuário, permitindo que até mesmo pessoas leigas em programação e tecnologia produzam com facilidade e agilidade imagens e vídeos adulterados (Moraes, 2020).

Dentre os vários aplicativos/programas disponíveis para *download*, pode-se listar como os mais populares: Zao, Wombo, DeepFaceLab, Reface, Deepfakes web, FaceSwap, FaceApp, FacePlay, FaceMagic e Anyface (Kinast, 2022). Em suma, todos disponibilizam a qualquer usuário da Internet a possibilidade de manipular imagens e/ou vídeos por meios de técnicas de *deepfake*. O Quadro 1 indica quais atividades cada aplicativo é capaz de desenvolver e sua disponibilidade.

Quadro 1: Principais aplicativos que disponibilizam técnicas de *deepfake*.

Aplicativos	Atividade	Disponibilidade
Zao	Permite construir uma personalidade cinematográfica e transferir rostos para personagens de um filme	Disponível para Android e iOS gratuitamente
Wombo	Permite criar vídeos de pessoas cantando por meio de uma fotografia, utilizando a sincronização labial	Disponível para Android e iOS gratuitamente
DeepFaceLab	Permite trocar faces, substituir a cabeça inteira, bem como alterar o movimento dos lábios	Disponível para Android e iOS gratuitamente
Reface	Permite criar vídeos <i>deepfake</i> , inserindo as características do rosto de uma fotografia em personagens de filmes ou programas de TV	Disponível para Android e iOS gratuitamente
Deepfakes web	Permite criar vídeos <i>deepfake</i> com melhor qualidade devido ao recurso de modelo de reutilização	Disponível via site mediante pagamento
FaceSwap	Permite trocar rostos em imagens e vídeos	Disponível via site gratuitamente
FaceApp	Permite realizar modificações e alterações faciais em fotografias	Disponível para Android e iOS gratuitamente
FacePlay	Permite trocar faces em fotos e vídeos de forma rápida	Disponível para Android e iOS gratuitamente
FaceMagic	Permite trocar faces vídeos modelo	Disponível para Android e iOS gratuitamente
Anyface	Permite trocar rosto e expressões faciais em imagens, além de gerar imagens falantes com frases pré-carregadas	Disponível para Android gratuitamente

Fonte: as autoras.

Entretanto, tantas inovações e possibilidades trazem consigo preocupações. São várias as possibilidades de ilícitos que podem ser cometidos com a utilização das técnicas de *deepfake*, entre eles: crimes contra a honra (arts. 138, 139 e 140 da Lei n.º 2.848/1990, Código Penal), crime de falsificação de documento particular, falsidade ideológica e estelionato (arts. 298, 299 e 171 da Lei n.º 2.848/1990, Código Penal), crime de perseguição (art. 147-A da Lei n.º 2.848/1990, Código Penal), crimes contra a dignidade sexual (arts. 213 a

234 da Lei n.º 2.848/1990, Código Penal) e crime de aliciamento de crianças (art. 241-D da Lei n.º 8.069/1990, Estatuto da Criança e do Adolescente).

Os agressores veem nas técnicas de *deepfake* uma oportunidade de se valer dos avanços tecnológicos para diversificar suas abordagens às vítimas. Uma das situações específicas em que a *deepfake* pode ser aplicada por pessoas com má intenção é o aliciamento de crianças e adolescentes. Cabe explicar que na literatura inglesa existem dois termos distintos para se referir ao aliciamento: *grooming* e *enticement*. O primeiro, *grooming*, é o procedimento sistemático e que exige tempo para construir confiança, manipular emocionalmente e isolar a vítima para obter submissão e cometer abusos (Santin *et al.*, 2012; Santin, 2013; Freitas; Barbosa; Santin, 2016). Já o segundo termo, *enticement*, é o ato específico de atrair ou seduzir uma criança ou adolescente, frequentemente usando presentes ou promessas para facilitar um ato sexual. O *grooming* é a preparação; o *enticement* é uma técnica dentro desse procedimento. Normalmente o termo *grooming* refere-se ao aliciamento realizado por meio da Internet.

Com isso, considerando que aliciadores também têm acesso às técnicas de *deepfake*, fez-se necessário compreender as normas brasileiras relativas à proteção de crianças e adolescentes, em especial no ambiente digital e identificar de que forma as técnicas de *deepfake* podem ser utilizadas pelos agressores para ludibriar e aliciar suas vítimas.

2. NORMATIVAS BRASILEIRAS E AS TÉCNICAS DE DEEPPFAKE

O Estatuto da Criança e do Adolescente (Lei n.º 8.069/1990 – ECA) é a principal normativa brasileira que ampara e defende os direitos destinados à infância e adolescência (Brasil, 1990). Elaborada com base nas premissas que constituem os direitos humanos, o ECA reconhece as crianças/adolescentes como cidadãos que possuem direitos fundamentais e direitos específicos, enfatizando a necessidade de desenvolver políticas públicas que possibilitem a proteção integral desse grupo no contexto em que estão inseridos. Destaca que é dever de todos prevenir a ocorrência de ameaça ou violação dos direitos das crianças e adolescentes, salientando inclusive o dever do Estado nessa

proteção. A partir de 17 de março de 2026, entrou em vigor o denominado ECA Digital (Lei n.º 15.211/2025) que alterou o texto normativo do ECA e ampliou a proteção legal ao ambiente digital, devendo ser aplicado a qualquer produto ou serviço digital que tenha como foco crianças e/ou adolescentes, menores de 18 anos, independentemente de onde esteja sediada a empresa que oferta tais serviços ou produtos. Finalmente, o ECA Digital veio para efetivamente transferir às plataformas digitais e respectivas empresas a responsabilidade ativa e obrigatória de proteger crianças e adolescentes no meio digital (Brasil, 2025).

Originalmente, o ECA tipifica o aliciamento de crianças no art. 241-D que abarca as seguintes condutas: aliciar, assediar, instigar ou constranger, através de qualquer meio de comunicação, criança com o fim de com ela praticar ato libidinoso. Esse artigo foi inserido no ECA por meio da Lei n.º 11.829/2008 (Brasil, 2008) e representou uma rígida modificação, uma vez que com a alteração legislativa a consumação do crime de aliciamento de crianças independe da prática dos atos libidinosos. Entretanto, foi criticado e não é bem aceito por parte da doutrina devido a uma brecha na redação ao não fazer menção aos adolescentes. Assim, só é possível punir por meio do art. 241-D do ECA o agente que praticar aliciamento contra pessoa de até 12 anos incompletos, conforme disposição do art. 2º, do mesmo diploma legal.

No que diz respeito às normas relativas a *deepfake*, por ser uma recente aplicação de técnicas de IA, ainda não existe legislação brasileira específica para regulamentar as questões relativas ao desenvolvimento e uso de técnicas de *deepfake*. Entretanto, já foram criadas normas que combatem os crimes praticados na rede mundial de computadores, entre elas se destacam a Lei n.º 12.737/2012 - Lei de Crimes Informáticos (Brasil, 2012), a Lei n.º 12.965/2014 (Marco Civil da Internet) (Brasil, 2014) e a Lei n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD (Brasil, 2018).

A Lei de Crimes Informáticos ficou conhecida popularmente como Lei Carolina Dieckmann, uma vez que a atriz poderia ter sofrido com a invasão de seus dispositivos informáticos e vazamento de conteúdo pessoal. Essa normativa, dentre outras providências, inseriu no Código Penal a tipificação de delitos informáticos por meio do art. 154-A chamado de crime de invasão de dispositivo informático. Foi um importante marco jurídico brasileiro, tendo em

vista ser uma das primeiras legislações a punir os crimes cibernéticos, sendo que antes da alteração legislativa a invasão de dispositivos privados era considerada atos preparatórios, portanto, práticas impuníveis. Apesar de ter garantido a evolução das legislações acerca do uso da Internet, foi considerada muito genérica por ser abrangente, sem especificar de forma precisa os delitos, carecendo de aprimoramentos que garantam clareza e aplicabilidade.

Decorrente de tais críticas, essa lei foi atualizada por meio das leis n.º 14.132/2021 (Brasil, 2021) e n.º 14.155/2021 (Brasil, 2021), alterando disposições acerca de diversos crimes, dos quais destaca-se os delitos de invasão de dispositivos informáticos, perseguição, furto mediante fraude eletrônica, estelionato mediante fraude eletrônica. Uma das principais mudanças foi a especificação de que o crime informático não mais necessita de quebra de mecanismos de segurança para assim ser caracterizado, admitindo formas variadas de execução. Antes da alteração legislativa, segundo alguns juristas, era necessário demonstrar a ocorrência de medida violenta ou a existência de mecanismo de segurança para configurar o crime, diferente disso a conduta seria atípica (Penido, 2013).

O Marco Civil da Internet regula o uso da Internet no Brasil com base em princípios, garantias, direitos e deveres, além de determinar as diretrizes para atuação do Estado em relação à matéria. Cabe ressaltar que o Marco Civil da Internet estabelece princípios importantes que se relacionam às aplicações de imagens/vídeos manipulados, tais como: liberdade de expressão (art. 3º, I), proteção da privacidade (art. 3º, II) e responsabilização dos agentes de acordo com suas atividades (art. 3º, VI). Ademais, consolida os direitos e garantias dos usuários da Internet, em especial quanto à inviolabilidade da intimidade, vida privada e das comunicações (art. 7º), bem como a responsabilidade por danos decorrentes de conteúdo gerado por terceiros (art. 18) (Brasil, 2014). Apesar desse dispositivo conter disposições que asseguram a proteção, por exemplo, de imagem, personalidade e honra, há uma lacuna no que diz respeito à aplicação de técnicas de *deepfake*.

Já a LGPD busca regulamentar o tratamento fornecido aos dados pessoais cedidos pelo próprio indivíduo àqueles que capturam informações pessoais sensíveis ou não sobre os usuários, seja por meio digital ou não. Nessa lei foram abordados os chamados dados pessoais sensíveis, que são aqueles

que merecem maior proteção por quem os coleta, armazena, trata e exclui. Os dados pessoais sensíveis são caracterizados por aqueles que geram a identificação do indivíduo ou aqueles que, quando cruzados, possam tornar o usuário identificável em termos de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, art. 7º da LGPD (Brasil, 2018). Objetiva, em especial, a proteção de direitos e dados pessoais da pessoa natural e a transparência de tratamento. Cabe destacar que reforça em seu art. 2º, inciso IV, no que tange à proteção de dados sensíveis como imagem e voz, a inviolabilidade dos direitos à honra e à imagem sob a perspectiva da proteção de dados. Dessa forma, a elaboração de imagens/vídeos manipulados somente poderia ocorrer de acordo com as hipóteses dispostas no art. 7º, entre elas, o consentimento do titular, para o cumprimento de obrigação legal e para proteção da vida.

Apesar da evolução na legislação brasileira acerca do uso da Internet, com diversos trechos que remetem à proteção do direito à imagem e personalidade no ambiente digital, ainda não há previsão expressa sobre aplicação de técnicas de *deepfake*. Na época em que essas leis foram promulgadas, ferramentas de IA voltadas a este tipo de aplicação sequer haviam sido desenvolvidas para aplicação em larga escala, estando restrita aos laboratórios de pesquisa. Com isso, percebe-se a necessidade de criar normativas que regulamentem expressamente as questões relativas ao desenvolvimento, colocação no mercado, supervisão e uso de sistemas de IA como um todo, destacando-se as técnicas de *deepfake*.

Como forma de preencher essa lacuna legislativa, diversos projetos de lei foram elaborados. Entre eles, foi desenvolvido pela deputada Rogéria Santos o Projeto de Lei n.º 2.709/2024 a fim de alterar o ECA incluindo o inciso VIII no art. 87 para determinar a realização de campanhas permanentes sobre os riscos dos conteúdos digitais, incluindo tecnologias para identificar e remover imagens ou vídeos adulterados com técnicas de *deepfake* e outros materiais, os quais envolvam violência e exploração sexual de crianças e adolescentes (Brasil, 2024). O deputado federal Saullo Vianna desenvolveu também o Projeto de Lei n.º 177/2024 que busca instituir a campanha de conscientização e prevenção

contra crimes cibernéticos, cometidos por meio do uso indevido de sistemas de IA, contra crianças e adolescentes (Brasil, 2024).

Observa-se tanto a preocupação com o tema quanto um movimento em coibir tais práticas por meio de projetos de lei. Foi elaborado pelo Senador Jorge Kajuru o Projeto de Lei n.º 1.272/2023 a fim de incluir no Código Penal o art. 308-A que tipifica a adulteração maliciosa de vídeos ou áudios (Brasil, 2023).

Destaca-se também o Projeto de Lei n.º 146/2024, elaborado pelo senador Chico Rodrigues, que inclui os §3º e §4º no art. 141 (crime de constrangimento ilegal) e o §1º no art. 307 (crime de falsa identidade), ambos do Código Penal (Brasil, 2024). Esse projeto de lei busca aumentar a pena nos crimes contra a honra cometidos em redes sociais que utilizem técnicas de *deepfake*. Além disso, procura majorar a pena do crime de falsa identidade para quem criar imagem ou vídeo falso com *deepfake* para atribuir falsa identidade a si ou a outra pessoa.

Outro projeto de lei relevante para a discussão é o elaborado pelo deputado federal Saullo Vianna, sob n.º 896/2024, que busca tipificar a criação, produção, disseminação, compartilhamento e comercialização de técnicas de *deepfake* com a intenção de difamar, enganar ou prejudicar indivíduos, especialmente crianças e adolescentes (Brasil, 2024). Além disso, estabelece que as plataformas digitais que veiculam imagens ou vídeos digitais adulterados com técnicas de *deepfake* com o intuito de difamar, enganar ou prejudicar indivíduos serão responsáveis por implementar mecanismos de detecção e remoção desses conteúdos.

No âmbito eleitoral e de proteção à mulher, destacam-se: (i) Projeto de Lei n.º 5.241/2023 que altera a Lei n.º 4.737, de 15 de julho de 1965, para tipificar o crime de divulgação de *deepfake* durante período de campanha eleitoral (Brasil, 2023); (ii) Projeto de Lei n.º 5.242/2023 (Brasil, 2023), o qual altera a Lei n.º 9.504, de 30 de setembro de 1997 (Brasil, 1997), e estabelece normas para eleições, para dispor sobre a vedação a criação, utilização e propagação de *deepfake* no âmbito eleitoral; e (iii) Projeto de Lei n.º 5.467/2023 (Brasil, 2023), o qual altera a Lei n.º 11.340, de 7 de agosto de 2006 - Lei Maria da Penha (Brasil, 2006), e o Código Penal (Brasil, 1940), para reconhecer que a divulgação de conteúdo falso sexual configura violência doméstica e familiar e

para criminalizar a divulgação de registro falso não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso.

Há que se comentar ainda sobre o Projeto de Lei n.º 2.338/2023 (Brasil, 2023), que visa regulamentar o uso de sistemas de IA no Brasil, de modo que Freitas (2025, p. 230-240) comenta que o referido PL adota o modelo de regulação baseado em riscos e as obrigações também incluem temas como avaliação e gestão de riscos, documentação de conformidade, governança, autorregulação e boas práticas, códigos de conduta, transparência, responsabilidade civil, prestação de informações e cooperação com autoridades, proteção de dados pessoais, cibersegurança, entre outros. Em especial, o art. 7º, inciso VII, em seu § 3º, aduz que “Os sistemas de inteligência artificial que se destinem a grupos vulneráveis, tais como crianças, adolescentes, idosos e pessoas com deficiência, serão desenvolvidos de tal modo que essas pessoas consigam entender seu funcionamento e seus direitos em face dos agentes de inteligência artificial”. O que demonstra uma preocupação para que os desenvolvedores busquem estabelecer interfaces explicativas e de fácil entendimento. Especificadamente, entende-se a partir do art. 14, inciso II, ao tratar de sistemas de IA de risco excessivo, que o PL veta a implementação e o uso de sistemas de IA que “explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como as associadas à sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial a sua saúde ou segurança ou contra os fundamentos desta Lei.”

Entretanto, espera-se que os inúmeros PLs sejam analisados, de modo que os criminosos, que se utilizam de técnicas de *deepfake* para ludibriar crianças e adolescentes, sejam devidamente punidos. Nesse sentido, se torna de extrema importância a criação de tipificação especial para os delitos cometidos por meio de técnicas de *deepfake*, levando em conta que a aplicação de analogia *in malam partem* é vedada pelo direito penal brasileiro.

3. IMPACTOS DA APLICAÇÃO DE TÉCNICAS DE DEEPFAKE PARA ALICIAMENTO DE CRIANÇAS E ADOLESCENTES NO DIREITO BRASILEIRO

Infelizmente, por se tratar de uma recente inovação tecnológica, a legislação brasileira não prevê especificamente leis aplicáveis para casos que envolvem o uso de técnicas de *deepfake* no aliciamento de crianças e adolescentes na Internet. Entretanto, existem outras normativas que podem ser aplicadas a esses casos, a depender da interpretação e da existência de evidências digitais que demonstrem e possam caracterizar prova não somente da aplicação de tais técnicas, mas da conduta dos aliciadores. Neste sentido, por não haver leis específicas, existem diversas lacunas que precisam ser regulamentadas.

No Brasil, o aliciamento pela Internet em si, independentemente da efetiva prática de ato libidinoso, é penalmente tipificado pelo ECA em seu art. 241-D, como apresentado anteriormente. Entretanto, conforme já abordado, a normativa possui uma lacuna ao não incluir os adolescentes no sujeito passivo do tipo, de modo que o aliciamento por meio digital, quando praticado contra pessoas com 12 anos ou mais, não possui tipificação penal.

Compreende-se desta situação que os legisladores entenderam que a partir dessa faixa etária os adolescentes teriam maturidade suficiente para lidar com a abordagem dos aliciadores e identificar possíveis criminosos *online*. Deste modo, os adolescentes não tenham sido incluídos na tipificação justamente porque não fazia sentido punir quem assedia uma pessoa nessa idade, já que o próprio ordenamento jurídico brasileiro prevê que ato libidinoso com maior de 14 anos de idade não configura crime de estupro de vulnerável (art. 217-A do Código Penal). Todavia, essa divergência nas idades existente entre as tipificações resulta em incongruência no ordenamento jurídico acerca de qual idade a pessoa passaria a ter discernimento e maturidade suficientes para fazer determinadas escolhas e separar uma tomada de decisão consciente ou identificar elementos caracterizadores de técnicas de *deepfake*.

É contraditório estabelecer que há presunção de violência na prática de atos libidinosos com pessoa menor de 14 anos de idade e não incluir essa faixa

etária na tipificação do crime de aliciamento, visto que o entendimento decorre de haver ou não maturidade para o consentimento. Mas diante da aplicação de técnicas de *deepfake*, não se está discutindo o aliciamento *versus* o consentimento, está se discutindo a aplicação de técnicas que servem para antes de tudo, inclusive ao aliciamento e abuso sexual, para ludibriar crianças e adolescentes. Inclusive, foi consolidado pela Súmula 593 do Superior Tribunal de Justiça que a presunção inerente ao crime de estupro de vulnerável é absoluta, “sendo irrelevante eventual consentimento da vítima para a prática do ato, sua experiência sexual anterior ou existência de relacionamento amoroso com o agente” (Brasil, 2017). Assim, nessa lógica, deveria de se presumir violência na prática de aliciamento e abuso sexual contra adolescentes de 12 a 13 anos, porém isso não acontece no ordenamento jurídico brasileiro.

Para além disto, há que se comentar que o ECA Digital menciona uma única vez o termo “inteligência artificial”, quando do Capítulo V – Da Supervisão Parental, em seu art. 17, inciso IV, § 4º, item VIII, explica que as configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo a “VIII – revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas.” (Brasil, 2025). De um modo geral, o ECA Digital transfere às plataformas digitais e respectivas empresas a responsabilidade ativa e obrigatória de proteger crianças e adolescentes no meio digital, visto serem tais plataformas e empresas as mais beneficiadas economicamente.

Por outro lado, o ECA Digital, mais uma vez se debruça e explicita como fundamento que a utilização de produtos ou serviços de tecnologia da informação (TI) por crianças e adolescentes deverá atentar para “a segurança contra intimidação, exploração, abuso, ameaça e outras formas de violência” (art. 4º, inciso IV) (Brasil, 2025). E, ainda, que tais fornecedores ou de acesso provável por crianças e adolescentes deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato

com conteúdos, produtos ou práticas de exploração e abuso sexual (art. 6º, inciso I) (Brasil, 2025).

Esta preocupação também está explícita no art. 27, de modo que, novamente, caberá aos fornecedores, em território nacional, “remover e comunicar os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados em seus produtos ou serviços, direta ou indiretamente, às autoridades nacionais e internacionais competentes” (Brasil, 2025). Interessante observar que o texto legislativo utiliza o termo “aparente”, ou seja, uma vez que são diversos os significados na língua portuguesa do Brasil, podendo referir-se a algo que aparece, que é visível ou evidente, mas pode ser também, algo que é parecido ou semelhante e, ainda, algo suposto, especioso ou enganador. Neste mesmo artigo do ECA Digital, o parágrafo 2º explicita que os fornecedores deverão reter, pelo prazo estabelecido no Marco Civil da Internet (art. 15) os dados associados a um relatório de conteúdo de exploração e de abuso sexual de criança ou de adolescente, podendo os fornecedores arcarem com as sanções estabelecidas no art. 35 (Brasil, 2025).

Ainda há que se comentar que o PL n.º 2.338/2023 poderá contribuir para coibir que sistemas de Inteligência Artificial que façam uso de técnicas de *deepfake* sejam destinados a grupos vulneráveis, tais como crianças e adolescentes, uma vez que categoriza tais sistemas como de risco excessivo e, portanto, veta a implementação e o uso de sistemas de IA que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, conforme arts. 7º e 14 (Brasil, 2023).

Finalmente, os diversos outros projetos de lei, comentados anteriormente, devem ser analisados com urgência, a fim de preencher as lacunas legislativas existentes no ordenamento jurídico brasileiro.

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar os limites do direito brasileiro para coibir ou mitigar os riscos de aliciamento de crianças e adolescentes por meio de técnicas de *deepfake*. Observou-se que a utilização de imagens/vídeos manipulados pode ser uma ferramenta poderosa e de fácil acesso para os criminosos a fim de auxiliar no aliciamento das prováveis

vítimas. Quando se trata de crianças e adolescentes a preocupação é ainda maior, devido ao pouco discernimento e inocência desse grupo, que facilita a atuação dos aliciadores.

Ao averiguar as normativas brasileiras acerca do tema, notou-se que embora o país possua legislação específica e abrangente para a proteção de crianças e adolescentes, como o ECA e o ECA Digital, ainda existem lacunas significativas quando se trata do uso de novas tecnologias para aliciar e abusar de crianças e adolescentes. Há que se estar atento para o fato de que, como discutido no artigo, o art. 241-D do ECA criminaliza o aliciamento de crianças, mas não estende essa proteção de forma adequada aos adolescentes, deixando uma área cinzenta na lei. Além disso, por se tratar de uma recente inovação tecnológica, não há menção específica ao uso de técnicas de *deepfake*, o que pode complicar ainda mais a identificação e a punição desses crimes, agora enfrentados também pelo ECA Digital, por meio das reflexões ora apresentadas.

Foi possível verificar que se faz necessária, com urgência, a elaboração de regulamentação específica para o uso de técnicas de *deepfake* no contexto do aliciamento de crianças e adolescentes. O Marco Civil da Internet e a LGPD fornecem um quadro geral para a proteção de direitos no ambiente digital, mas não abordam as nuances específicas da *deepfake*, deixando para o ECA Digital e o PL n.º 2.338/2023 o enfrentamento da questão.

Com base nas discussões apresentadas, conclui-se que há uma lacuna significativa na legislação brasileira em relação à proteção de crianças e adolescentes diante do uso de técnicas de *deepfake* para aliciamento. A criação e aprovação de leis específicas que abranjam essa tecnologia, em especial quando aplicadas contra crianças e adolescentes, são essenciais para garantir uma proteção jurídica eficaz. A tramitação urgente de projetos de lei que preencham essas lacunas legislativas é fundamental para garantir a segurança e o bem-estar de crianças e adolescentes na era digital, no ambiente digital.

Em suma, a pesquisa reflete a necessidade de se olhar para uma problemática específica, mas de altíssimo risco, buscando-se apontar as lacunas e o entrelaçamento de legislações no ordenamento jurídico. Espera-se, portanto, uma atualização legislativa contínua que acompanhe a evolução tecnológica, garantindo que o ordenamento jurídico brasileiro seja capaz de responder adequadamente às novas formas de atuação da criminalidade que

surgem com o avanço das tecnologias digitais que afetam, nos casos mais graves relacionados ao aliciamento e ao abuso sexual, o desenvolvimento da personalidade de crianças e adolescentes, sua saúde física e mental.

REFERÊNCIAS

AFCHAR, D. *et al.* **MesoNet: a Compact Facial Video Forgery Detection Network**. IEEE International Workshop on Information Forensics and Security (WIFS). Hong Kong, China: IEEE, dez. 2018. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8630761>. Acesso em: 03 mar. 2026.

ASSEMBLEIA LEGISLATIVA DO ESTADO DE MINAS GERAIS. **Reunião de Comissão, 16/05/2024, 14:00**. Disponível em: <https://www.almg.gov.br/atividade-parlamentar/comissoes/reuniao/?idTipo=2&idCom=1132&dia=16&mes=05&ano=2024&hr=14:00>. Acesso em: 01 mar. 2026.

BALLARD, D. H.; BROWN, C. M. **Computer Vision**. Prentice-Hall, 1982.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 03 mar.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18069.htm. Acesso em: 01 mar. 2026.

BRASIL. **Lei n.º 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/14737compilado.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 11.340, de 07 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera os Decretos-Lei n.º 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei n.º 7.210, de 11 de julho de 1984 (Lei de Execução Penal); e dá outras providências (Lei Maria da Penha). Brasília, DF: Presidência da República,

2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111340.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 11.829, de 25 de novembro de 2008**. Altera a Lei n.º 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Brasília, DF: Presidência da República, 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/111829.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 01 mar. 2026.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 01 mar. 2026.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 14.132, de 31 de março de 2021**. Acrescenta o art. 147-A ao Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei n.º 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114132.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei n.º 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm. Acesso em: 03 mar. 2026.

BRASIL. **Lei n.º 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da

Criança e do Adolescente). Senado Federal, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 03 abr. 2026.

BRASIL. **Projeto de Lei n.º 1.272, de 2023**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940, para criar o crime do art. 308-A – adulteração maliciosa de vídeos ou áudios. Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/156383#tramitacao_10455615. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Senado Federal, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>. Acesso em: 03 mar.

BRASIL. **Projeto de Lei n.º 5.241, de 2023**. Altera a Lei n.º 4.737, de 15 de julho de 1965, para tipificar o crime de divulgação de deep fake durante período de campanha eleitoral. Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2399786>. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 5.242, de 2023**. Altera a Lei n.º 9.504, de 30 de setembro de 1997, para dispor sobre a vedação à criação, utilização e propagação de deep fake. Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2399792>. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 5.467, de 2023**. Altera a Lei n.º 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal). Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2403507>. Acesso em: 03 mar.

BRASIL. **Projeto de Lei n.º 146, de 2024**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena para os crimes contra a honra e hipótese qualificada para o crime de falsa identidade, para quando houver a utilização de tecnologia de inteligência artificial para alterar a imagem de pessoa ou de som humano. Senado Federal, 2024. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161947>. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 177, de 2024**. Institui a Campanha de Conscientização e Prevenção contra Crimes Cibernéticos, cometidos por meio do uso indevido da inteligência artificial, contra crianças e adolescentes. Câmara dos Deputados, 2024. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2417362>. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 896, de 2024**. Dispõe sobre a Proteção contra Deepfakes e dá outras providências. Câmara dos Deputados, 2024. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2422375>. Acesso em: 03 mar. 2026.

BRASIL. **Projeto de Lei n.º 2.709, de 2024**. Altera a Lei n.º 8.069, de 12 de julho de 1990 (Estatuto da Criança e do Adolescente) para determinar a realização de campanhas permanentes sobre os riscos dos conteúdos digitais que envolva a violência e exploração sexual de crianças e adolescentes. Câmara dos Deputados, 2024. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2445631>. Acesso em: 03 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula n.º 593**. Diário da Justiça, Brasília, DF, 2017. Disponível em:

<https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=593.num>. Acesso em: 03 mar. 2026.

FREITAS, C. O. A. **Direito e Não-Coisas**. 1º. ed., Rio de Janeiro: Lumen Juris, 2025.

FREITAS, C. O. A.; BARBOSA, C. M.; SANTIN, P. L. L. Aliciamento sexual de crianças e adolescentes na internet sob a perspectiva da teoria da comunicação ludibriante. **Revista Magister de Direito Penal e Processual Penal**, v. 70, p. 13–32, 2016.

GOTTFREDSON, L. S. Mainstream science on intelligence: An editorial with 52 signatories, history, and bibliography. **Intelligence**, v. 24, n. 1, p. 13–23, jan. 1997.

HAUGELAND, J. **Artificial intelligence: The very idea**. MIT press, 1985.

KINAST, P. **10 melhores apps e sites para deep fake**. Oficina na net, 2022. Disponível em: <https://www.oficinadanet.com.br/aplicativos/43136-apps-sites-deep-fake>. Acesso em: 03 mar. 2026.

KUMAR, G. N. C. **Artificial intelligence: Definition, types, examples, technologies**. Medium, 2018. Disponível em: <https://chethankumargn.medium.com/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b>. Acesso em: 03 mar. 2026.

KURZWEIL, R. **The Age of Spiritual Machines**. Massachusetts: The MIT Press, 1990.

MASOOD, M. *et al.* Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. **Applied intelligence**, v. 53, n. 4, p. 3974–4026, 2023.

MORAES, C. P. “Deepfake” como ferramenta de manipulação e disseminação de “fakenews” em formato de vídeo nas redes sociais. **Biblios (Peru)**, n. 79, 2020.

NORVIG, P.; RUSSELL, S. Inteligência artificial. **Rio de Janeiro: Grupo GEN**, 2013.

OLSON, L. N. *et al.* Entrapping the innocent: Toward a theory of child sexual predators’ luring communication. **Communication Theory**, v. 17, n. 3, p. 231–251, 2007.

PENIDO, F. **Os crimes previstos na Lei Dieckmann**. Olhardireito, 2013. Disponível em:
<https://www.olhardireito.com.br/artigos/exibir.asp?id=5846&artigo=os-crimes-previstos-na-lei-dieckmann%3E>. Acesso em: 03 mar. 2026.

POOLE, D. I.; GOEBEL, R. G.; MACKWORTH, A. K. **Computational intelligence**. Oxford University Press New York, 1998.

RASHID, A. The Talk of Crime. **Investigative Practice Journal**, p. 28–29, 2008.

SANTIN, P. L. L. **Análise automática de textos de mensagens instantâneas para detecção de aliciamento sexual de crianças e adolescentes**. 2013. Dissertação (Mestrado em Informática) – Pontifícia Universidade Católica do Paraná, Curitiba, 2013.

SANTIN, P. L. L. *et al.* Modelagem de Aliciamento de Menores em Mensagens Instantâneas de Texto. **Anais do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2012)**, Porto Alegre: SBC, v. 1, p. 288–301, 2012. Disponível em:
<https://secplab.ppgia.pucpr.br/files/papers/2012-3.pdf>. Acesso em: 03 mar. 2026.

SHAH, M. Guest introduction: the changing shape of computer vision in the twenty-first century. *International Journal of Computer Vision*, v. 50, p. 103–110, 2002.

SKANSI, S. **Introduction to deep learning**: from logical calculus to artificial intelligence. Switzerland: Springer, 2018 (e-book).

SMOLA, A.; VISHWANATHAN, S.V.N. **Introduction to machine learning**. United Kingdom: Cambridge University Press, 2008.

SOUZA, V.; HELDER, D. **Deepfake ao vivo**. G1, 2023. Disponível em: <https://surl.lt/ykwovz>. Acesso em: 01 mar. 2026.

STAIR, R. M. *et al.* **Princípios de sistemas de informação**. Cengage Learning, 2021.

WINSTON, P. H. **Artificial intelligence**. Addison-Wesley Longman Publishing Co., Inc., 1992.

TAXONOMIA CREDIT

Daniele Deidio: Conceituação, Curadoria de dados, Análise Formal, Investigação, Redação do manuscrito original.

Cinthia Obladen de Almendra Freitas: Conceituação, Metodologia, Administração do projeto, Supervisão, Redação - revisão e edição.