DIREITO
V.9 • N.3 • 2024 - Fluxo Contínuo

ISSN Digital: **2316-381X**
ISSN Impresso: **2316-3321**
DOI: **10.17564/2316-381X.2024v9n3p343-355**

INTERFACES CIENTÍFICAS

DEEPFAKE PORNOGRÁFICO NA SOCIEDADE DE RISCO CONTEMPORÂNEA: OS DESAFIOS DE REGULAMENTAÇÃO E CONTROLE DA INTELIGÊNCIA ARTIFICIAL

PORNOGRAPHIC DEEPFAKES IN CONTEMPORARY RISK SOCIETY: CHALLENGES IN REGULATING AND CONTROLLING ARTIFICIAL INTELLIGENCE

ULTRAFALSOS (DEEPFAKES) PORNOGRÁFICOS EN LA SOCIEDAD DE RIESGO CONTEMPORÁNEA: RETOS EN LA REGULACIÓN Y CONTROL DE LA INTELIGENCIA ARTIFICIAL

Lucas Ribeiro de Faria1
Lucas Gonçalves da Silva2
Henrique Ribeiro Cardoso3

RESUMO

Este artigo analisa o problema do *Deepfake* pornográfico na sociedade moderna, quando imagens e vídeos íntimos e falsos, na maioria dos casos tendo mulheres como vítimas, são compartilhados na *internet*. Busca-se aferir se o cenário atual na utilização de inteligência artificial aumenta o risco social. O problema foi considerado relevante em razão do aumento na disponibilização de ferramentas de inteligência artificial que, cada vez mais, estão mais acessíveis ao público em geral e adquirindo capacidade de gerar conteúdo praticamente indistinguível da realidade. Através do método de pesquisa dogmático e com a análise de decisões judiciais e notícias divulgadas na mídia, pretende-se analisar se existe alguma forma de regulação criminal, cível ou tecnológica eficaz no uso das ferramentas disponíveis na *internet* para que menos conteúdo pornográfico falso seja gerado e, principalmente, compartilhado. O trabalho foi desenvolvido com o método dedutivo.

PALAVRAS-CHAVE

Deepfake. Pornografia. Sociedade de risco. Inteligência artificial.

ABSTRACT

This article examines the issue of pornographic deepfakes in modern society, where intimate and false images and videos, mostly victimizing women, are shared on the internet. The aim is to assess whether the current use of artificial intelligence enhances social risk. The problem has become relevant due to the increasing availability of AI tools that are becoming more accessible to the general public and capable of generating content that is virtually indistinguishable from reality. Through a doctrinal research method and analysis of judicial decisions and media reports, the study intends to explore whether there is any effective criminal, civil, or technological regulation in place for using internet tools to reduce the generation and, primarily, the dissemination of false pornographic content. The study was conducted using a deductive method.

KEYWORDS

Deepfake; pornography; Risk Society; Artificial Intelligence.

RESUMEN

Este artículo analiza el problema de los ultrafalsos (deepfakes) pornográficos en la sociedad moderna, donde imágenes y videos íntimos falsificados, que en su mayoría victimizan a mujeres, se comparten en internet. El objetivo es evaluar si el uso actual de la inteligencia artificial aumenta el riesgo social. Este problema ha cobrado relevancia debido a la creciente disponibilidad de herramientas de inteligencia artificial, cada vez más accesibles al público en general y capaces de generar contenido prácticamente indistinguible de la realidad. A través de un método de investigación doctrinal y del análisis de decisiones judiciales y reportes de medios, este estudio pretende explorar si existen regulaciones efectivas en materia penal, civil o tecnológica para limitar la creación y, sobre todo, la difusión de contenido pornográfico falso. La investigación se llevó a cabo utilizando un enfoque deductivo.

PALABRAS CLAVE

Ultrafalso. Deepfake. Pornografía. Sociedad de riesgo. Inteligencia artificial.

1 INTRODUÇÃO

O presente trabalho tem o propósito de explorar os aspectos do problema dos *Deepfakes* pornográficos e propor possíveis soluções, entretanto, devendo ser considerado que ainda se trata de tema recente diretamente ligado ao uso irresponsável de inteligência artificial.

Na metodologia do presente trabalho foi empregada a análise dogmática, com análise de livros, artigos e notícias publicados na *internet,* princípios jurídicos, normas aplicáveis, decisões judiciais e leis relacionadas à criação de conteúdo falso, que possuem o potencial de influenciar na forma que está sendo tratada essa questão.

Este artigo está organizado em cinco capítulos. No primeiro capítulo foi abordado como a sociedade moderna e digital evoluiu para um estado de constante transformação, emergindo novos riscos constantes e coletivos, a exemplo dos *Deepfakes* pornográficos. É abordado o progresso tecnológico que tornou possível a criação de *Deepfakes,* especialmente com a utilização de inteligência artificial, algoritmo que evolui empregando técnicas de autocorreção e aprendizagem profunda.

O segundo e o terceiro capítulos preocuparam-se em analisar a aplicação da tecnologia de *Deepfake* na produção de conteúdo pornográfico e abordar as consequências legais e sociais dos *Deepfakes* pornográficos, com a análise de como o conteúdo falso divulgado pode prejudicar a honra e a imagem das vítimas, especialmente tutelados pela Constituição Brasileira de 1988.

Por fim, o quarto capítulo preocupou-se com a discussão acerca das dificuldades de controlar e regular a criação e disseminação de *Deepfakes*, com a propositura de soluções e medidas preventivas para mitigar o problema.

Em síntese, o presente artigo busca proporcionar uma compreensão razoavelmente abrangente e detalhada acerca do problema dos *Deepfakes* Pornográficos, com uma abordagem metodológica dedutiva.

2 A SOCIEDADE DE RISCO E A INTELIGÊNCIA ARTIFICIAL

A sociedade de risco surge, dentre outros exemplos, como decorrência da percepção de riscos ecológicos, conflitos na distribuição de renda, imprevisibilidade das ameaças provocadas pelo desenvolvimento técnico-industrial (Beck, 1995).

Portanto, em uma sociedade de risco, fruto da globalização e da desconstrução das instituições que causavam as certezas sociais, ninguém está seguro. A própria sociedade introjeta e alimenta o risco, descaracterizando categorias sociais com a criação de novas categorias autofágicas.

Zygmunt Bauman, analisando o mesmo fenômeno, optou por chamá-lo de "Pós-Modernidade", que seria equivalente ao fenômeno dos estudos sobre Modernidade Reflexiva conduzidos por Ulrich Beck. Segundo Bauman (1999), a Pós-Modernidade é a Modernidade reconhecendo sua própria impossibilidade, mas reconhecendo, também, sua necessidade de automonitoramento e de conscientemente descartar o que outrora fazia inconscientemente.

Em uma modernidade contemporânea, não há mais a percepção do risco. Os que geram o risco também estão sujeitos ao risco gerado, considerando a integração mundial de um contexto ecológico, de um sistema político e de uma economia globalizados (Cardoso, 2010)

Saliente-se que o advento da Rede Mundial de Computadores, conhecida como *internet*, contribui sobremaneira para a integração de um mundo cada vez mais conectado e globalizado. A ferramenta, de inegável alcance e com potencial facilitador da vida humana, entretanto, também viabiliza um aumento exponencial da exposição ao risco, seja causado por si, seja causado por terceiros, o que deve ser objeto de análise.

O aumento do acesso à *internet* torna praticamente ilimitada a possibilidade de transmissão de informações, salvo regulações específicas em certos países. Além da possibilidade de acesso a conteúdo do mundo inteiro, a capacidade de disseminação é exponencial, podendo ocorrer de determinada prática ou conteúdo aumentar seu conhecimento – ou reprodução – de forma exponencial.

O avanço da tecnologia faz parte do Século XXI. Com a popularização do acesso à *internet*, hoje mundialmente estabelecida, todos têm acesso a uma infinidade de informações nos dispositivos eletrônicos. O uso da tecnologia está integrado ao cotidiano do ser humano que, no afã de resolver problemas existentes ou imaginados, utiliza da sua criatividade para desenvolver novas ferramentas de produtividade, formas de lazer, armas de guerra, técnicas de manejo agrícola, tecnologias de informática, dentre outras áreas.

No bojo das tecnologias criadas surge a Inteligência Artificial (I)A, espécie de algoritmo senciente que, por meio de programação, consegue simular uma consciência pensante, com o objetivo primordial de ajudar nas tarefas humanas. Segundo Russel (2013), ao citar outros autores renomados da área, é possível extrair das inteligências artificiais a definição de computadores que pensam, podendo perceber, raciocinar, agir e executar funções que exigem inteligência quando executadas por pessoas.

Para definir a existência de uma inteligência artificial, é possível aplicar o "Teste de Turing", proposto por Alan Turing em 1950, sendo que o computador (aqui, conceito empregado de forma ampla) deve passar por uma série de indagações realizadas por um examinador humano que, após as respostas, não deve ser capaz de saber se foram geradas por um ser humano ou por uma inteligência artificial (Russel, 2013).

As inteligências artificiais, além do avanço possibilitado pela atividade humana, também se aperfeiçoam à medida que são utilizadas, já que os algoritmos, programações básicas em código, não só possibilitam a inteligência artificial como a aperfeiçoa a cada novo erro por ela produzida (Lessa; Cabral; Silvestre, 2020).

O avanço da inteligência artificial contemporânea, entretanto, permite muito mais do que a geração espontânea de textos. Os mecanismos já são capazes de reconhecer objetos, realizar conversas fluidas que emulam a experiência humana, gerar imagens complexas e até vídeos ultrarrealistas, utilizando as faces de pessoas que não originariamente gravaram aquele conteúdo.

São ferramentas dotadas de tamanho poder não apenas de processamento de informação, mas, principalmente, de criação de informação, vídeos com imagens falsas começam a ser gerados por inteligências artificiais, de forma dolosa e por meio de intervenção humana, sem corresponderem realmente às gravações reais feitas com as pessoas que aparecem nos vídeos.

2 O SURGIMENTO DE *DEEPFAKES*

A inteligência artificial contemporânea é capaz não apenas de processar grande volume de informações e interagir de forma senciente, simulando a consciência humana, mas também de criar conteúdo em forma de imagens e vídeos de praticamente qualquer objeto ou ser vivo.

As inteligências artificiais modernas também já conseguem criar vídeos a partir de imagens pré-existentes de pessoas, alterando o conteúdo de fala, simulando voz ou mesmo transmutando a face de uma pessoa para o corpo de outra pessoa.

Tais vídeos, com identidades falsas, falas ou ações que nunca ocorreram, são definidos como *Deepfakes*:

> *Deepfakes* são, essencialmente, identidades falsas criadas com o Deep Learning [aprendizagem profunda, por meio de uso maciço de dados], por meio de uma técnica de síntese de imagem humana baseada na inteligência artificial. É usada para combinar e sobrepor imagens e vídeos preexistentes e transformá-los em imagens ou vídeos "originais" [...] Essa combinação de vídeos existentes e "originais" resulta em vídeos falsos, que mostram uma ou algumas pessoas realizando ações ou fazendo coisas que nunca aconteceram na realidade. Em 2019, também estamos vendo uma explosão de faces fake, através das quais a IA é capaz de conjurar pessoas que não existem na realidade, e que têm um certo fator de fluência. (Spencer, 2019, n.p.).

Diversos *Deepfakes* já tiveram uma ampla disseminação e repercussão, inclusive a nível mundial, quando vídeos falsos envolvendo personalidades famosas foram criados com a intenção de ludibriar as pessoas, especialmente em relação a falas que nunca ocorreram.

A título de exemplo, personalidades como Barack Obama (ex-presidente dos Estados Unidos da América), Volodymyr Zelensky (Presidente da Ucrânia) e Mark Zuckerberg (criador do *Facebook*) já foram alvos de *Deepfakes*, em vídeos extremamente realistas (Canaltech, 2022), criados por inteligência artificial, que possuem falas nunca proferidas na realidade.

Por outro lado, alguns *Deepfakes* são criados com motivação claramente voltada ao entretenimento, como a utilização de rostos e vozes de famosos ou personalidades públicas em filmes já lançados (Canaltech, 2022).

Como se percebe, o grande risco do *Deepfake* reside no seu grau de verossimilhança, na medida em que as vozes e imagens geradas por inteligência artificial em vídeo são tão próximas da realidade que, se referentes a um assunto de grande seriedade ou relevância, podem ludibriar um imenso número de pessoas com assuntos muito sérios, especialmente com a facilidade de propagação de informações que a *internet* proporciona atualmente.

Os algoritmos de inteligência artificial estão avançando de forma vertiginosa, capazes de gerar conteúdo mais realista após cada autocorreção, sem a necessidade de intervenção humana para a melhoria gráfica dos vídeos e fotos gerados:

> Já é sabido que o algoritmo de criação dos *deepfakes* possui um aprendizado profundo que analisa e prevê automaticamente, corrigindo prováveis erros. Tem-se a inteligência artificial

> produzindo máquinas capazes de utilizar o conhecimento e a linguagem de uma forma bem próxima da que o ser humano realiza. A inteligência artificial caminha cada vez mais rápido, permitindo que a ciências da computação crie suas máquinas com capacidade de inteligência cada vez mais próxima à realidade do homem. Da mesma forma que os seres humanos utilizam a cognição e a linguagem para evoluir e comunicar, a inteligência artificial busca através de seus algoritmos que as funções cognitivas e comunicativas humanas, sejam reproduzidas pelos programas virtuais. (Lessa; Cabral; Silvestre, 2020, p. 483)

A verossimilhança do *Deepfake* possui, dessa forma, um risco duplo: primeiro, lida-se com a potencial desinformação que atinge àqueles que consomem o conteúdo falso; segundo, existe uma violação ao direito de imagem da pessoa que teve sua fala, suas expressões faciais e suas ações modificadas.

Por outro lado, em relação às vítimas do *Deepfake* que possuem suas imagens alteradas em vídeos e fotos, infelizmente percebe-se o surgimento de *Deepfakes* pornográficos, com vítimas predominantemente mulheres, onde vídeos ou fotos falsas são divulgados com um extremo nível de realismo e com conteúdo sexual, sem que aquela pessoa que protagoniza o vídeo ou que apareceu na foto tenha praticado qualquer ato sexual registrado por câmeras.

A título de exemplo, em 2021, uma mulher chamada Jodie (nome fictício) foi vítima de *Deepfake,* quando vídeo que continha seu rosto no corpo de outra mulher, que fazendo sexo com vários homens ao mesmo tempo, foi divulgado na *internet*. Jodie narrou que foi vítima diversas vezes de informações digitais inverídicas e os severos abalos psicológicos que sofreu em razão desses acontecimentos (BBC News, 2024).

Da mesma forma, Kate Isaacs, mulher que se intitula “ativista contra o pornô de vingança”, foi alvo de *Deepfake* com um vídeo pornográfico, quando seu rosto foi inserido digitalmente no corpo de outra mulher (G1, 2022). Kate deixou claro que ser algo de *Deepfake* impactou severamente em sua saúde e causou problemas psicológicos para confiar em outras pessoas.

O problema afeta qualquer mulher que tenha sua imagem acessível, de alguma forma, na *internet.* A primeira-ministra italiana, Giorgia Meloni, também foi alvo de *Deepfake* pornográfico, pedindo na justiça uma indenização de 100 mil euros em processo aberto contra dois homens que supostamente sobrepuseram seu rosto em corpos de mulheres que atuaram em vídeos pornográficos (CNN, 2024).

O *Deepfake* pornográfico foi reconhecido, inclusive, pela Polícia Civil do Estado de Sergipe como um problema grave, em razão da possibilidade de utilizar as imagens falsas para “convencer uma pessoa a passar dados pessoais acreditando que está falando com outra pessoa”, viabilizando um estelionato eletrônico, ou de utilização na “produção de conteúdo falso de pornografia” (Polícia Civil [...], 2023).

A criação de *Deepfake* pornográfico já é uma realidade acessível à maioria das pessoas em razão do avanço e da popularização da inteligência artificial, sem a necessidade de conhecimento ou habilidade específica.

3 A POTENCIALIZAÇÃO DO RISCO SOCIAL E A DIFICULDADE DE CONTROLE OFENSA AOS DIREITOS CONSTITUCIONAIS À HONRA E À IMAGEM

O direito constitucional à honra possui caráter subjetivo, estando ligado ao valor moral do sujeito, a seu nome, a sua consideração social e até a sua fama, refletindo a dignidade pessoal perante os outros e a forma como a pessoa é enxergada no meio social (Fernandes, 2017). Já o direito à imagem pode ser considerado em uma dupla acepção: a "imagem-retrato", que seria o direito à reprodução gráfica da imagem do sujeito, ou a "imagem-atributo", por sua vez, relacionada à imagem do sujeito no contexto do meio social (Fernandes, 2017).

Tratam os direitos à honra e à imagem de direitos de personalidade, que abarca tanto o direito à esfera íntima, secreta e privada quanto ao direito de autodeterminação, por sua vez de auto localização no tempo e no espaço em relação à própria sexualidade ou às próprias informações (Canotilho, 2018).

A utilização de Deepfake pornográfico, considerando a disseminação de imagens ou vídeos falsos em que constam a fisionomia de uma pessoa que nunca praticou determinado ato sexual gravado, visto que a pornografia é associada à ausência de moralidade, tem o potencial de macular a honra e a imagem (imagem-atributo) da pessoa atingida.

É atual a discussão acerca da necessidade de regulamentação desse tipo de ferramenta para diminuir o risco social, considerando que o Deepfake pornográfico é feito por meio de inteligência artificial:

> Pode-se falar, em resumo, que a necessidade de legislação a respeito da IA se relaciona intrinsecamente com a noção de garantia da segurança jurídica e digital, a minimização dos riscos a todos os envolvidos, a exigência de transparência, ética e respeito aos direitos humanos e fundamentais. (Melo Júnior; Oliveira, 2023, p.101)

O *Deepfake* pornográfico, desta forma, engloba indubitavelmente direitos de ordem constitucional erigidos ao *status* de garantias fundamentais, na medida em que ofende em larga escala (transmissão contínua e facilitada na *internet*) a honra e imagem de um indivíduo.

Em razão do cenário exposto, surge a necessidade de tutelar corretamente as garantias fundamentais, que asseguram ao indivíduo que teve seus direitos violados que exija do Poder Público, inclusive do Poder Judiciário, o respeito ao direito violado que instrumentaliza a garantia (Mendes, 2017).

Todavia, referida tutela do Poder Público enquanto mantenedor da garantia esbarra em maior dificuldade com o *Deepfake* pornográfico criado por inteligência artificial: primeiro, em razão da atual facilidade de criação e; segundo, devido à facilidade de compartilhamento do conteúdo indesejado, que em poucas horas pode atingir um número indeterminado de pessoas, sendo impossível garantir que seja completamente extirpado da *internet*, mesmo após determinação judicial.

Desta forma, é extremamente pertinente discutir como regulamentar o uso da inteligência artificial e quais mecanismos de controle para a criação e divulgação de *Deepfakes* devem ser empregados pelo Poder Público e pelas empresas que exploram serviços ligados ao uso da *internet*, com o objetivo de impedir a perpetuação de mídias inverídicas de cunho sexual que atingem, sobretudo, as mulheres.

4 A NORMATIVIZAÇÃO PENAL E A REGULAÇÃO DO USO DE INTELIGÊNCIAS ARTIFICIAIS SÃO RESPOSTAS AO PROBLEMA?

No atual momento, não existe no ordenamento jurídico brasileiro uma figura típico-normativa específica para punir, com a utilização do direito penal, o *Deepfake* de conteúdo pornográfico cometido contra vítima do sexo feminino. A conduta é atualmente enquadrada como violência psicológica contra a mulher, prevista no art. 147-B do Código penal, inserido em 28 de julho de 2021 pela Lei nº 14.188/2021, que entrou em vigor na data de sua publicação.

Depreende-se que a conduta, apesar de não ser atípica devido à possibilidade de enquadramento do núcleo verbal fático no tipo penal normativo, é punida com pena de reclusão de somente seis meses a dois anos, se não constituir crime mais grave.

O delito não necessariamente é cometido no contexto da Lei nº 11.340/2006 (Lei Maria da Penha), considerando que exige uma situação de convivência doméstica ou familiar contra a mulher e de vulnerabilidade, segundo o Superior Tribunal de Justiça, no julgamento do Agravo Regimental no Agravo em Recurso Especial n. 1.700.032/GO, hipótese em que não seria admitida suspensão condicional do processo ou a transação penal, de acordo com a Súmula 536 do Superior Tribunal de Justiça.

Fora os casos de violência doméstica, não existe qualquer impedimento para que os casos que apurem o cometimento do delito previsto no art. 147-B do Código Penal viabilizem, por exemplo, a suspensão condicional do processo, eis que atendidos os requisitos do art. 89 da Lei nº 9.099/1995.

Igualmente, o art. 76 da Lei nº. 9.099/1995 pode ser aplicado aos casos de violência psicológica contra a mulher que não estejam tutelados pela Lei Maria da Penha, tornando possível a celebração de transação penal. Aplicada a pena privativa de liberdade, é possível que seja realizada a substituição por pena restritiva de direitos, conforme art. 44 do Código Penal, considerando que a pena não é superior a quatro anos e que o crime não é cometido com violência ou grave ameaça à pessoa, e contanto que não haja reincidência, devendo o condenado possuir culpabilidade, antecedentes, conduta social e personalidade favoráveis, em caráter subjetivo, sendo a substituição suficiente em relação aos motivos e circunstâncias.

Ademais, mesmo que executada a pena privativa de liberdade, seu cumprimento ocorre em regime aberto, a teor do art. 33, §1º, alínea "c", do Código Penal Brasileiro. A insuficiência da tutela penal motivou a apresentação de projetos de lei, tanto no âmbito da Câmara dos Deputados quanto no Senado Federal, tipificando a conduta criminalmente.

A Câmara dos Deputados está tramitando o Projeto de Lei nº 5.467/2023, de autoria da Deputada Federal Camila Jara, que acrescentaria o art. 216-C ao Código Penal Brasileiro, para prever pena de detenção de seis meses a um ano, e multa, para aquele que divulgar conteúdo falso sexual, por qualquer meio, com cena de nudez ou ato sexual ou libidinoso sem autorização da vítima. Caso o delito seja praticado contra menor de idade, a pena seria de reclusão de um a três anos e multa.

Por outro lado, no Senado Federal, o Senador Weverton (PDT/MA) apresentou o Projeto de Lei nº 5.721/2023, propondo também a inserção do art. 216-C no Código Penal Brasileiro, entretanto, com

pena mais dura de reclusão de um a três anos, podendo ser aumentada de um terço a dois terços se o crime for praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com a finalidade de vingança ou de humilhação.

Esses movimentos do Poder Legislativo revelam uma lacuna normativa da legislação criminal para tutelar o problema do *Deepfake* pornográfico, considerando que o direito penal brasileiro se preocupa em proteger bens jurídicos de igual relevância ou até menos relevantes em outros crimes tipificados no Código Penal e na legislação criminal extravagante.

A Constituição Federal tutela, como exposto, os direitos à honra e à imagem do indivíduo. Entretanto, no âmbito do *Deepfake*, torna-se necessário averiguar se existem mecanismos preventivos e repressivos que tornem real a possibilidade de lidar com o problema. O conteúdo gerado por uma ferramenta de inteligência artificial pode ser detectado por outra ferramenta de inteligência artificial, contanto que existam programações antagônicas (uma de criação, uma de detecção).

A título de exemplo, a rede social Meta (antigo *Facebook*) lançou, em 05 de abril de 2024, uma ferramenta automática de identificação de conteúdo gerado por inteligência artificial para imagens, vídeos e áudios, com aplicabilidade imediata em todas as redes sociais do grupo Meta, que engloba também as redes sociais *Instagram* e *Threads* (Meta [...], 2024).

Especificamente em relação à rede social *Instagram*, foi adicionada a opção para que o próprio usuário rotule o conteúdo como criado por inteligência artificial (opção "Rotular como IA"), trazendo às pessoas uma espécie de responsabilidade compartilhada para que aquele conteúdo publicado seja claramente exposto como gerado por um algoritmo (Techtudo, 2024).

Percebe-se um certo movimento, mesmo que ainda recente e pequeno, de viabilizar um maior controle do conteúdo falso criado e divulgado na *internet*, podendo-se citar como exemplo recente projeto de lei apresentado no Congresso dos Estados Unidos da América (Instituto Humanitas Unisinos, 2024), intitulado "*Take it down*", cujo objetivo é penalizar rigorosamente pessoas e empresas de tecnologia que deixem de remover o conteúdo de *Deepfake* pornográfico dentro do prazo legalmente ou judicialmente estabelecido.

No Brasil, já foi promulgada a Lei nº 12.965/2014, conhecida como Marco Civil da *Internet*, existindo no artigo 19 uma previsão expressa de responsabilização civil por danos gerados se o provedor responsável pela hospedagem do conteúdo, após ordem judicial, não tomar as providências necessárias para removê-lo no prazo determinado.

5 CONCLUSÃO

É possível concluir que a legislação brasileira, lentamente mutável, ainda não está preparada para lidar com esse problema moderno. Apesar de existirem algumas bases principiológicas capazes de lidar com os direitos fundamentais envolvidos, existe uma latente necessidade de reforçar e de adaptar as ações do Poder Público (legiferantes e judicantes) para coibir a criação e a disseminação de *Deepfakes*.

Ademais, é necessário refletir acerca da necessidade de criar penalidades claras para os infratores e mecanismos eficazes para a remoção rápida do conteúdo ilegal da *internet*. A legislação deve incluir medidas preventivas para que os provedores de conteúdo estejam obrigados a verificar a integridade do conteúdo compartilhado, no escopo de evitar a disseminação de conteúdo falso, questão atualmente possível com a utilização e desenvolvimento de tecnologias de detecção avançada.

Em relação à utilização internacional da *internet*, com *uploads* de conteúdo e acesso em qualquer lugar do mundo, é essencial que mecanismos de colaboração internacional também sejam implementados. Ações coordenadas entre países podem ser fundamentais para estabelecer padrões e regulamentos comuns, além de facilitar a troca de informações e tecnologias de detecção.

As redes sociais e os *websites* de hospedagem de mídia, com o desenvolvimento de ferramentas como verdadeiras inteligências artificiais que fiscalizam outras inteligências artificiais, podem implementar uma análise automatizada de qualquer conteúdo compartilhado, de forma que o vídeo ou a foto, acaso tenha indícios de falsificação, fique com seu compartilhamento temporariamente suspenso enquanto uma checagem mais aprofundada é realizada.

Outro aspecto diz respeito a possível vitimização, visto que o problema dificilmente será completamente extirpado. É de suma importância que as plataformas de mídia social e outros serviços *on-line* adotem políticas de apoio às vítimas na denúncia e remoção de conteúdos ofensivos. Além disso, uma rede de apoio deve ser criada para que a vítima tenha acesso a serviços de suporte psicológico, técnico e jurídico para ajudá-las a lidar com as consequências da disseminação de conteúdos falsos.

Por fim, é essencial que as empresas de tecnologia sejam responsabilizadas pelo uso indevido de suas plataformas e ferramentas. Tal responsabilização não pode – e não deve – recair sobre o usuário. Devem ser implementadas políticas rigorosas de uso e desenvolvimento de tecnologias que dificultem a criação e disseminação de conteúdo falso. Ademais, devem colaborar com autoridades e organizações de direitos humanos para monitorar e combater o uso indevido de suas tecnologias.

Enfrentar o problema dos *Deepfakes* pornográficos requer uma abordagem multidisciplinar que combine legislação clara, conscientização pública, colaboração internacional, inovação tecnológica e apoio às pessoas vitimadas. Somente por meio de esforços coordenados e contínuos será possível proteger os direitos fundamentais na era moderna e garantir que os avanços da inteligência artificial sejam utilizados para o benefício da sociedade, e não como uma ferramenta de abuso e violação dos direitos humanos.

REFERÊNCIAS

10 *DEEPFAKES* mais impressionantes que confundiram a *internet*. Canaltech, 2022. Disponível em: https://canaltech.com.br/internet/deepfakes-mais-impressionantes-que-confundiram-a-internet-219962/. Acesso em: 27 maio 2024.

BAUMAN, Zygmunt. Modernidade e ambivalência. Tradução: Marcus Penchel. Rio de Janeiro: Jorge Zahar Editor, 1999.

BECK, Ulrick; GIDDENS, Anthony; LASH, Scott. Modernização reflexiva: **política, tradição e estética na ordem social moderna.** Trad. Magda Lopes. São Paulo: Universidade Estadual Paulista, 1997.

BITTAR, Eduardo C. B. O direito na pós-modernidade. Rio de Janeiro: Forense Universitária, 2014.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.467**, de 2023. Autoria da Deputada Federal Camila Jara. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2358932. Acesso em: 27 jun. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jun. 2024.

BRASIL. Senado Federal. **Projeto de Lei do Senado nº 5.721**, de 2023. Autoria do Senador Weverton (PDT/MA). Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9514433&ts=1701272265579&disposition=inline. Acesso em: 27 jun. 2024.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Agravo em Recurso Especial n. 1.700.032 - GO. Nome das partes. Relator: Ministro Ribeiro Dantas, julgado em 09 dez. 2020. Quinta Turma, Diário da Justiça Eletrônico, Brasília, DF, 14 dez. 2020. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202001081490&dt_publicacao=14/12/2020. Acesso em: 26 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 536**. Segunda Seção. Publicada em 10 de setembro de 2014. Disponível em: https://scon.stj.jus.br/SCON/sumstj/toc.jsp?livre=%27536%27.num.&O=JT. Acesso em: 27 jun. 2024.

CANOTILHO, J. J. Gomes *et al*. Comentários à Constituição do Brasil. 2. ed. São Paulo: Saraiva Educação, 2018.
CARDOSO, Henrique Ribeiro. Controle da legitimidade da atividade normativa das agências reguladoras. Rio de Janeiro: Lumen Juris, 2010.

DEEPFAKE: Colocaram meu rosto em um vídeo pornô. G1, 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/10/21/deepfake-colocaram-meu-rosto-em-um-video-porno.ghtml. Acesso em: 30 maio 2024.

FERNANDES, Bernardo Gonçalves. Curso de Direito Constitucional. 9. ed. rev. atual. ampl. Salvador: JusPodivm, 2017.

FUI COLOCADA em *deepfake* pornô pelo meu melhor amigo. BBC NEWS, 2024. Disponível em: https://www.bbc.com/portuguese/articles/cev992wp5zwo. Acesso em: 30 maio 2024.

I*NDIA'S GENERAL election is being impacted by Deepfakes*. Le Monde, 2024. Disponível em: https://www.lemonde.fr/en/pixels/article/2024/05/21/india-s-general-election-is-being-impacted-by-deepfakes_6672168_13.html?utm_source=the_news&utm_medium=newsletter&utm_campaign=24-05-2024. Acesso em: 30 maio 2024.

INSTAGRAM: como usar novo recurso que rotula conteúdos como IA. **TechTudo**, 2024. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/2024/05/instagram-como-usar-novo-recurso-que-rotula-conteudos-como-ia-edapps.ghtml. Acesso em: 27 junho 2024.

LESSA, Moyana Mariano Robles; CABRAL, Hildeliza Lacerda Tinoco Boechat; SILVESTRE, Gilberto Fachetti. *Deepfake*: **a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. Revista Jurídica Derecho y Cambio Social**, n. 61, p. 475-487, jul./set. 2020.

MELO JÚNIOR, José Eustáquio de; OLIVEIRA, Gustavo Paschoal Teixeira de Castro. **Contributos da logística para a elaboração do marco legal da inteligência artificial no Brasil. Revista de Informação Legislativa: RIL**, Brasília, DF, v. 60, n. 237, p. 99-114, jan./mar. 2023. Disponível em: https://www12.senado.leg.br/ril/edicoes/60/237/ril_v60_n237_p99. Acesso em: 27 maio 2024.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 12. ed. rev. atual. São Paulo: Saraiva, 2017.

META IDENTIFICARÁ conteúdos gerados por IA em suas redes sociais. **Meio e Mensagem**, 2024. Disponível em: https://www.meioemensagem.com.br/midia/meta-identificara-conteudos-gerados-por-ia-em-suas-redes-sociais. Acesso em: 27 junho 2024.

POLÍCIA CIVIL do Estado de Sergipe. **Inteligência artificial acende alerta para crimes de pornografia e vingança com imagens falsas criadas com *Deepfake*.** 2023. Disponível em: https://www.policiacivil.se.gov.br/inteligencia-artificial-acende-alerta-para-crimes-de-pornografia-e-vinganca-com-imagens-falsas-criadas-com-deepfake/. Acesso em: 30 maio 2024.

RUSSELL, Stuart J. Inteligência artificial. Trad. Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

SENADOR apresenta projeto que combate pornografia fake nos EUA. **Instituto Humanitas Unisinos**, 2024. Disponível em: https://www.ihu.unisinos.br/categorias/640683-senador-apresenta-projeto-que-combate-pornografia-fake-nos-eua. Acesso em: 30 julho 2024.

SPENCER, Michael K. *Deep Fake*, a mais recente ameaça distópica. Tradução de Gabriela Leite. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/. Acesso em: 20 maio 2024.

Recebido em: 28 de Agosto de 2024
Avaliado em: 14 de Setembro de 2024
Aceito em: 22 de Outubro de 2024

A autenticidade desse artigo pode ser conferida no site https://periodicos.set.edu.br

1 Especialista em processo penal; pós-graduado em Ciências Criminais; Mestrando em Direito pelo Programa de Pós-Graduação da Universidade Federal de Sergipe – UFS; Advogado. E-mail: lucasrfaju@gmail.com.

2 Doutor e Mestre em Direito do Estado pela PUC/SP; Pós-doutor em Direito pela Università Degli Studi G. d'Annunzio (Itália) e pela Universidade Federal da Bahia – UFBA; Professor Associado da Graduação em Direito e do Programa de Mestrado em Direito na Universidade Federal de Sergipe – UFS. E-mail: lucasddi@academico.ufs.br

3 Doutor e Mestre em Direito, Estado e Cidadania, pela Universidade Gama Filho – UGF/RJ; Especialista em Direito Constitucional Processual pela Universidade Federal de Sergipe – UFS (FAPESE/UFS); Professor do Programa de Pós-Graduação stricto sensu (Mestrado) e da graduação da Universidade Federal de Sergipe – UFS.
E-mail: henriqueddi@academico.ufs.br

GRUPO TIRADENTES
Inspirando o futuro
EDUNIT