LUMEN ET VIRTUS
ISSN: 2177-2789

DESAFIOS PARA A SEGURANÇA E PROTEÇÃO DE DADOS NO MEIO DIGITAL

CHALLENGES FOR SECURITY AND DATA PROTECTION IN THE DIGITAL ENVIRONMENT

DESAFÍOS PARA LA SEGURIDAD Y LA PROTECCIÓN DE DATOS EN EL ENTORNO DIGITAL

https://doi.org/10.56238/levv16n53-142

Data de submissão: 01/10/2025 **Data de publicação:** 31/10/2025

Marcos Vinícius Silva de Brito
Acadêmico do curso de Bacharelado em Direito
Instituição: Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma
E-mail: msilvadebrito25@gmail.com

Pedro Silva Mendes
Pós-graduado em Docência do Ensino Superior
Instituição: Universidade Anhanguera Uniderp
E-mail: pedro.mendes@unisulma.edu.br

RESUMO

O progresso da inteligência artificial tem implementado transformações significativas em diversos setores da sociedade, inclusive no campo jurídico, onde surgem novos paradigmas que devem ser enfrentados pela sociedade, sobretudo quanto a segurança e proteção de dados no meio digital em tempos de uso de deepfake. Nota-se que, a análise desse fenômeno é essencial para entender as consequências jurídicas e éticas, e também para propor soluções tecnológicas e legais. O presente estudo tem como objetivo analisar como a disseminação de deepfakes compromete a integridade das informações e impacta os direitos fundamentais como a privacidade, a honra e a liberdade de expressão. A metodologia utilizada foi definida como pesquisa é do tipo exploratória e abordagem qualitativa, tendo como meio de pesquisa a revisão bibliográfica da literatura. Para concretização do estudo, foram realizados levantamentos de material online e em meio físico, inserindo-se nesta revisão, fontes de artigos, livros, documentos normativos governamentais, jurisprudência, notícias atuais e citação de casos práticos. Os resultados evidenciaram que o uso de deepfakes afeta de sobremaneira os direitos da personalidade, que não constitui um direito em si, mas são as permissões dadas pelo ordenamento jurídico que possibilita que cada pessoa possa tutelar a vida. As soluções até agora encontradas, é enquadras as ações criminosas conforme os resultados produzido, como calúnia, injúria e difamação, estelionato eletrônico, e/ou mesmo o uso da Lei Geral de Proteção de dados – LGPD.

Palavras-chave: Inteligência Artificial. Proteção de Dados. Deepfakes. Direitos Fundamentais.

ABSTRACT

The advancement of artificial intelligence has brought about significant transformations in various sectors of society, including the legal field, where new paradigms emerge that must be addressed, especially regarding data security and protection in the digital environment in times of deepfake use. It is important to note that analyzing this phenomenon is essential to understanding the legal and ethical

consequences, as well as to proposing technological and legal solutions. This study aims to analyze how the spread of deepfakes compromises the integrity of information and impacts fundamental rights such as privacy, honor, and freedom of expression. The methodology used was exploratory research with a qualitative approach, using a bibliographic review as the research tool. To complete the study, we surveyed online and physical material, including sources such as articles, books, government regulatory documents, case law, current news, and case studies. The results showed that the use of deepfakes significantly affects personality rights, which are not rights in themselves, but rather the permissions granted by the legal system that allow each person to protect their life. The solutions found so far are to classify criminal actions according to the results produced, such as slander, libel, and defamation, electronic fraud, and/or even the abuse of the General Data Protection Law (LGPD).

Keywords: Artificial Intelligence. Data Protection. Deepfakes. Fundamental Rights.

RESUMEN

El avance de la inteligencia artificial ha generado transformaciones significativas en diversos sectores de la sociedad, incluyendo el ámbito jurídico, donde emergen nuevos paradigmas que la sociedad debe abordar, especialmente en lo que respecta a la seguridad y protección de datos en el entorno digital ante el uso de deepfakes. Se destaca que el análisis de este fenómeno es esencial para comprender las consecuencias legales y éticas, así como para proponer soluciones tecnológicas y jurídicas. Este estudio analiza cómo la difusión de deepfakes compromete la integridad de la información e impacta derechos fundamentales como la privacidad, el honor y la libertad de expresión. La metodología empleada fue una investigación exploratoria con enfoque cualitativo, utilizando una revisión bibliográfica como método de investigación. Para llevar a cabo el estudio, se recopilaron materiales tanto en línea como impresos, incluyendo artículos, libros, documentos normativos gubernamentales, jurisprudencia, noticias de actualidad y citas de casos prácticos. Los resultados mostraron que el uso de deepfakes afecta significativamente los derechos de la personalidad, los cuales no son derechos en sí mismos, sino permisos otorgados por el sistema legal que permiten a cada persona proteger su vida. Las soluciones encontradas hasta el momento implican clasificar las acciones delictivas según los resultados obtenidos, como la calumnia, la difamación, el fraude electrónico e incluso la aplicación del Reglamento General de Protección de Datos (RGPD).

Palabras clave: Inteligencia Artificial. Protección de Datos. Deepfakes. Derechos Fundamentales.

1 INTRODUÇÃO

Na contemporaneidade, observa-se, mas do que nunca, uma transformação social promovida pelo avanço tecnológico, reconfigurando as dinâmicas sociais, culturais e econômicas. Assim, a convergência entre inteligência artificial, aprendizado de máquina e processamento de dados em larga escala, tem proporcionado uma verdadeira revolução digital, emergindo a partir disso, novos paradigmas. Assim, o tema - Desafios para a segurança e proteção de dados no meio digital- é extremamente relevante no cenário atual, considerando o aumento exponencial do uso de tecnologias digitais e a crescente quantidade de dados pessoais e sensíveis armazenados e processados em plataformas online.

Nos últimos anos, o avanço tecnológico proporcionou uma transformação digital em praticamente todos os setores, como a educação, a saúde, o comércio e as relações de trabalho. Com isso, a circulação de dados no ambiente virtual se tornou massiva. Empresas, governos e indivíduos dependem de sistemas digitais para suas atividades, o que também aumentou a exposição a riscos de segurança cibernética.

Nesse sentido, a disseminação de fakes envolvendo a manipulação de vídeos e áudios, em que uma pessoa parece estar falando como se fosse outra, é uma questão preocupante e cada vez mais comum com o avanço da tecnologia. Isso envolve o uso de deepfakes, um tipo de tecnologia que utiliza inteligência artificial (IA) e aprendizado de máquina para criar vídeos, áudios ou imagens extremamente realistas, mas falsificados, onde o rosto e a voz de uma pessoa podem ser sobrepostos ao corpo ou fala de outra. Entende-se, portanto, que Deepfake é um termo derivado de "*deep learning*" (aprendizado profundo) e "*fake*" (falso). Ele se refere a uma técnica de IA usada para criar conteúdo falsificados, geralmente vídeos e áudios, que aparentam ser extremamente reais (Affonso, 2021). Essas ferramentas utilizam redes neurais e algoritmos complexos para imitar a aparência e a voz de uma pessoa. Por exemplo, um vídeo pode mostrar alguém dizendo coisas que nunca disse, e com a ajuda de tecnologias de síntese de voz, a manipulação pode parecer ainda mais convincente.

Essa tecnologia é baseada em Redes Neurais Generativas Adversariais (GANs), que criam imagens e áudios falsos treinando modelos em grandes conjuntos de dados reais. A GAN tem duas partes: uma rede geradora, que cria o conteúdo falso, e uma rede discriminadora, que tenta identificar se o conteúdo é falso ou real. O processo continua até que a rede discriminadora seja incapaz de diferenciar o conteúdo falso do real.

A investigação sobre a disseminação de deepfakes e seus impactos na integridade das informações e nos direitos fundamentais nesta pesquisa, justifica-se pela crescente ameaça que essa tecnologia representa para a segurança digital, a confiança pública e a democracia. Com o avanço da inteligência artificial e do aprendizado de máquina, os deepfakes tornaram-se uma ferramenta potente para a criação de vídeos e áudios falsificados que podem ser usados para desinformar, caluniar, fraudar

e manipular, afetando diretamente a privacidade, a honra e a liberdade de expressão das vítimas. Ademais, o uso mal-intencionado de deepfakes em contextos políticos, econômicos e pessoais pode gerar danos irreparáveis à reputação de indivíduos e instituições, influenciando eleições, processos judiciais e até mesmo a estabilidade social.

Portanto, a análise desse fenômeno é essencial para entender as consequências jurídicas e éticas, e também para propor soluções tecnológicas e legais que possam conter os efeitos negativos dos deepfakes, garantindo a proteção dos direitos fundamentais no ambiente digital e preservando a integridade da informação em uma era cada vez mais dominada pela tecnologia.

Nesse contexto, o estudo tem como objetivo, analisar como a disseminação de deepfakes compromete a integridade das informações e impacta os direitos fundamentais como a privacidade, a honra e a liberdade de expressão.

2 METODOLOGIA

A pesquisa é do tipo exploratória e abordagem qualitativa, tendo como meio de pesquisa a revisão bibliográfica da literatura. Para consumação do estudo, foram realizados levantamentos de material online e em meio físico, inserindo-se nesta revisão, fontes de artigos, livros, documentos normativos governamentais, jurisprudência, notícias atuais e citação de casos práticos relacionados ao tema. A opção pela revisão da literatura ocorreu em razão de se tratar de tema inovador, pouco regulamentando e que estar em constante evolução.

3 A TECNOLOGIA DEEPFAKE E SEU FUNCIONAMENTO

3.1 CONCEITO DE DEEPFAKE: ORIGEM DO TERMO E BASE TECNOLÓGICA (IA, REDES NEURAIS, GANS)

O termo *deepfake* nasce da combinação das palavras *deep learning* (aprendizado profundo) e *fake* (falso). Assim, nota-se que se trata de uma técnica de manipulação da mídia que se utiliza de algoritmos de Inteligência Artificial, sobretudo de Redes Neurais Artificiais, que identificam e aprendem padrões de traços humanos, realizando uma junção de imagens e áudios sobre determinado indivíduo, culminando em conteúdos audiovisuais realistas sobre a pessoa que é alvo. Assim, tornou-se usual a reprodução de rostos com voz de pessoas (Schereiber, Ribas e Mansur, 2020).

Diante os avanços tecnológicos, o *deepfake* pode ser criado com diferentes níveis de sofisticação, chegando a alcançar níveis extremamente convincentes dado o realismo empregado, sendo de difícil detecção visual. Nesse contexto, para que se alcance resultados otimizados, é preciso que a Inteligência Artificial se utilize de uma grande quantidade de informações disponíveis em bancos de dados (Beschizza, 2019).

Dado esse fenômeno, aponta-se que este ganhou maior atenção no ano de 2017 quando um usuário fez mal uso dessa tecnologia, criando conteúdos adultos falsos, utilizando-se de uma técnica de aprendizado de máquina chama de Redes Generativas Adversariais (Generative Adversarial Networks – GANs) permitindo a criação de conteúdo falso com alto grau de convencimento. No entanto, ressalte-se que esta tecnologia já existia, sendo fortemente mais utilizada na última década, sendo objeto de preocupação, levantando questões legais e éticos que envolvem esse tema (Novello, 2023).

Quanto ao seu funcionamento, observa-se que um deepfake geralmente exige o treinamento de um modelo de Rede Neural com um grande conjunto de dados de entrada, ou seja, exige um grande banco de dados que contenha vídeos, áudios e imagens da pessoa, sendo capaz de aprender os padrões dos traços e detalhes humanos daquela pessoa alvo, incluindo características faciais, suas expressões e outros detalhes, tais como a adaptação da luz ao rosto da pessoa e tom de voz (Figueira, 2020).

Dado esse contexto, com a reunião dessas informações o modelo de Rede Neural atua em duas frentes distintas, um gerador de conteúdo falso e um discriminador, no caso desse último, tem o objetivo de tentar distinguir a mídia real daquela que é falsa, conforme os padrões analisados, cabendo ao discriminador o apontamento daquilo que não se equipara a mídia real.

3.2 APLICAÇÕES POSITIVAS E NEGATIVAS

Diante do cenário de uso para prática de crimes, há de salientar-se que em contraste a esse cenário negativo, a *Deepfake* possui usos benéficos como a utilização em chats para experiências realistas, uso em realidade virtual, facilitação da acessibilidade e outras inúmeras possibilidades visuais que engloba a indústria artística de produções de multimídia (Novello, 2023).

Atualmente, dada a facilidade de acesso, ao contrário da sua produção que envolve uma complexa teoria, na prática cada vez mais torna-se mais fácil o acesso a essas ferramentas por meio de aplicativos que criam e manipulam a mídia artificial. Embora o uso indevido tenha causado preocupação no âmbito jurídico/social, essa ferramenta por ser usada em diversas áreas de forma positiva, como criar vídeos para conscientização social em diversos temas, como campanhas educativas (Figueira, 2020).

Na medicina pode ser aplicada para realização de pesquisa sem a necessidade de pacientes reais, e na educação pode ser empregada para auxílio ao aprendizado, com criação de vídeos históricos com personagens já falecidos. Ademais, essa ferramenta pode ter finalidade artística como a criação de vídeos realistas em museus. Soma-se a isso o uso no campo da publicidade, com criação de anúncios muito mais atraentes para o consumidor, gerando um maior impacto em vendas em razão da maior visibilidade dos produtos (Martínez et al, 2024).

Dada essa capacidade, recentemente, a Volkswagen lançou campanha com a cantora Elis Regina, que faleceu em 1982 e sua filha Maria Rita onde ambas interpretaram a canção -Como nosso País-, sendo esta campanha um marco no uso de deepfake no Brasil, pois gerou discussões sobre a ética e autenticidade. Nesse sentido, o uso dessa técnica *post mortem* suscita debates futuros no ordenamento jurídico nos próximos anos, incluindo situações do uso de voz e imagens de pessoas falecida, o que em tese pode ferir o princípio da vontade manifestada e levanta debate sobre direitos autorais (Novello, 2023).

Diante ao exposto, nota-se que, mesmo que a criação de *Deepfakes* exija expertise e técnica, além do aprendizado de máquina, nota-se que não parece distante o momento em que tais requisitos de criação serão superados e tornar-se-á cada vez mais otimizados esse processo, levantando preocupações acerca da disseminação sem controle desses conteúdos além do seu uso benéfico (Doffman, 2019).

3.3 EXEMPLOS RECENTES DE USO POLÍTICO, MIDIÁTICO E CRIMINAL

À medida que as aplicações das *deepfakes* se diversificaram, englobando à área de entretenimento, propagando política e a desinformação, podendo inclusive implicar em penalização criminal, cresceram as preocupações sobre seu potencial uso e os riscos e benefícios da sua utilização (Chagas e Moraes, 2023).

No contexto eleitoral, os *deepfakes* apresentam-se como uma ameaça real e significativa, podendo ser utilizada para criar e disseminar desinformação tendo objetivo de influenciar o comportamento dos eleitores durante o pleito. Logo, a manipulação dessa tecnologia pode induzir os eleitores a erro, fazendo-os a acreditar que determinados candidatos falaram coisas que nunca aconteceram, o que dificulta que sejam desmentidas posteriormente (Filho, Marrafon e Medón, 2022).

Nota-se, portanto, que essa tecnologia é uma ameaça multifacetada à integridade dos processos democráticos, trazendo novos desafios ao já complexo panorama eleitoral. Assim, a difamação de candidatos por *deepfakes* é um problema grave, que pode minar irremediavelmente a reputação das vítimas, contaminando o debate público (Hashioka, Silva e Marchetto, 2025).

Outra nuance eleitoral significativa quanto ao uso errôneo dessa tecnologia é a desacreditação das eleições, ou seja, por meio da disseminação de informações falsas, é possível desencorajar a participação cívica, o que por si, pode comprometer a representatividade do processo democrático, o que culmina por alterar os resultados eleitorais (Tavares, 2024). Conforme relatório anual da *Sumsub Identity Fraud Report* que analisa tendências e estatísticas globais de fraude de identidade, o Brasil apresentou crescimento de 830% em uso de deepfake entre os anos de 2022 e 2023 (Security Report, 2025).

Esses dados acendem alerta importante quanto ao mal uso eleitoral dessa tecnologia, recentemente, uma candidata à prefeitura de Bauru no Estado de São Paulo, Suéllen Rosim foi vítima do uso de deepfake, onde apareceu em vídeo erótico em véspera da eleição municipal, causando constrangimento e manipulando a opinião pública.

Celebridades como Pedro Bial, Drauzio Varella, William Bonner são alguns nomes de famosos que já foram vítimas de deepfake onde aparecia os seus rostos com o intuito de vender produtos de qualidade duvidosa. No caso de William Bonner o vídeo simulava uma reportagem do Jornal Nacional que tratava de dinheiro esquecido em bancos e suposta liberação imediata de crédito para o público (Miyashiro, 2024).

Ademais, além do uso político, dada a sua capacidade de reprodução realista, as *deepfakes* também desperta debates sobre os direitos da personalidade, como a privacidade, imagem e reputação do indivíduo. Nesse diapasão, saliente-se que a base teórica que sustentou o surgimento do direito à privacidade, estar centrada no fato que o indivíduo tem a opção de revelar informações a seus respeitos ou não.

Dessa forma, A Lei Maior de 1988 em seu art. 5º inciso X traz os direitos à personalidade como direitos essenciais, como à dignidade e integridade, sendo invioláveis.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988, p. 5).

Diante o exposto da hiperexposição vivenciado no Brasil e no mundo, no ano de 2018 foi criada a Lei Geral de Proteção de Dados (Lei. 13.709/18) que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Essa norma foi a responsável por prevê respeito a privacidade e inviolabilidade da intimidade, honra e imagem das pessoas com maior detalhamento, pois, quando há má-fé na exposição de dados sensíveis dos indivíduos, há clara violação desses direitos de privacidade (Ávila e Corazza, 2022).

Diante dessas constatações normativas, verifica-se que o uso de *deepfakes* torna-se um mecanismo ameaçador ao direito à privacidade de diversas formas, causando danos à reputação e à vida das vítimas. Assim, visando apresentar melhor detalhamento sobre a afetação das *deepfakes* sobre os direitos fundamentais das pessoas, serão realizado aprofundamento em capítulo específico a seguir:

4 DIREITOS FUNDAMENTAIS AFETADOS PELA DISSEMINAÇÃO DE DEEPFAKES

O uso de deepfakes afeta de sobremaneira os direitos da personalidade, que não constitui um direito em si, mas são as permissões dadas pelo ordenamento jurídico que possibilita que cada pessoa possa tutelar a vida, liberdade, identidade, a própria imagem a honra entre outros.

4.1 DIREITO À PRIVACIDADE

O direito à privacidade é visto como um pilar dos próprios direitos humanos e também do direito civil. Esse direito norteia-se pelo entendimento que os indivíduos têm o direito de manter traços de sua vida pessoal, longe do alcance do escrutínio público. Logo, enxerga-se na privacidade uma parte fundamental da própria dignidade e autonomia dos indivíduos, possibilitando que estes controlem informações sobre si e determinem como as informações são utilizadas (Tartuce, 2019).

Por sua importância, percebe-se que o direito à privacidade estar expresso também no Art. 21 do Código Civil de 2002, possuindo a seguir redação "vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". Assim, esse direito estar intimamente relacionado à vida íntima familiar, o que é atingida frontalmente quando há o mal uso de deepfakes, uma vez que o uso dessa tecnologia pode atingir a reputação e a vida privada das pessoas. Além disso, a violação perpetrada pelo uso de deepfake atinge também a proteção dos dados pessoais, pois a criação de conteúdo envolve diretamente a manipulação de imagens e áudios da vítima.

4.2 DIREITO À HONRA E IMAGEM

De acordo com Tartuce (2019) a honra é um valor que se relaciona à boa reputação, ou seja, o respeito que uma pessoa pode desfrutar na sociedade. Nesse contexto, o direito à honra relaciona-se a imagem pública, reputação e integridade moral. Logo, a proteção da honra de uma pessoa é essencial para preservação da sua dignidade.

Cabe destacar que, doutrinariamente, a honra pode adotar um contexto subjetivo e outro objetivo. A honra subjetiva trata da própria autoestima da pessoa, ou seja, é aquilo que ela pensa de si mesmo. Enquanto a honra objetiva abarca a ideia da repercussão social, ou aquilo que os outros pensam de algum indivíduo.

Nesse sentido, o uso de deepfake pode atingir a honra das pessoas com a criação de conteúdos difamatórios, como vídeos, e imagens que apresentação a pessoa em situação comprometedora, levando terceiros a acreditar em algo irreal. Além disso, deepfakes também pode enquadrar-se no âmbito da calúnia quando o conteúdo trata da falsa imputação de crime a terceiros.

4.3 LIBERDADE DE EXPRESSÃO E SEUS LIMITES NO AMBIENTE

A liberdade de expressão é um dos pilares das sociedades modernas, prevista no art. 5º, inciso IV da Carta Maior de 1988, assegura a manifestação do pensamento como um direito essencial, inerente ao exercício da cidadania. Logo, esta liberdade proporciona a diversidade de opiniões, a fiscalização dos poderes e desenvolvimento sociocultural. Porém, com o surgimento das novas tecnologias digitais, a informação passou a ser transformada em golpes e conteúdos falsos (Carvalho, 2022).

Essa nova dinâmica informacional tem se tornado um desafio para o ordenamento jurídico, uma vez que coloca em questão os limites da liberdade de expressão e o combate à desinformação. No Brasil esse processo tem se tornado um fenômeno grave, impactando processos eleitorais e contribu8indo para polarização de espectros políticos (Ventura, 2021).

Tratando-se dos limites da liberdade de expressão, Streck e Oliveira (2021) aponta que esse direito deve estar alinhado à veracidade e à confiabilidade das informações, sendo assim, os casos onde se utilizam de fake News, como o uso de deepfakes que ferem outros direitos das vítimas, como a intimidade, honra entre outros, não devem ser vistos como liberdade de expressão, mas como crimes que devem ser enfrentados sob o rigor da lei.

Nesse sentido, no Brasil é reconhecido o valor da liberdade de expressão, mas não é possível confundir essa liberdade com o direito de praticar crimes. Nesse sentido, o Marco Civil da Internet (Lei nº 12.965/2014) é considerado um avanço importante no estabelecimento de direitos sobre uso responsável da internet, ficando expresso que os provedores de conteúdo só podem ser responsáveis em caso de ilícitos, quando não realizarem a remoção de conteúdos após decisão judicial (Sarmento, 2020).

Assim, ao que parece, o legislador preocupou-se em preservar a liberdade de expressão ao mesmo tempo que criou mecanismos de remoção de conteúdos falsos como deepfakes entre outros. No entanto, saliente-se que é preciso muita moderação na remoção de conteúdos, tendo em vista que o excesso pode configurar censura prévia, o que pode prejudicar o Estado Democrático, sendo plausíveis os mecanismos do Marco Civil.

5 IMPACTOS JURÍDICOS E ÉTICOS DOS DEEPFAKES

Nesse capítulo aborda-se sobre os possíveis enquadramentos jurídicos do crime praticado sob uso de deepfakes e trata-se dos desafios para tipificação e aplicação das normas vigentes quanto aos crimes de manipulação digital.

5.1 POSSÍVEIS ENQUADRAMENTOS JURÍDICOS

Buscando a preservação dos Estado Democrático de Direito, atualmente, há um desafio crucial no Brasil, qual seja a responsabilização no cenário de deepfakes. Observa-se que a criação de deepfakes que retratam os indivíduos de maneira difamatória ou prejudicial pode causar sérios risos à imagem e reputação das pessoas, muitas vezes causando danos irreparáveis. A exemplo disso, cita-se vídeo de deepfake utilizado na última eleição presidencial onde mostrava-se enganosamente no jornal nacional, um resultado de pesquisa eleitoral falso, onde utilizava-se do rosto e da fala do apresentador William Bonner (Oliveira e Ávila, 2022).

Nesse sentido, a garantia do direito à imagem é um enorme desafio nos dias atuais. Assim, visando a melhor contextualização da tipificação de possíveis crimes que envolvem deepfakes e preciso entender o surgimento das primeiras normas relacionadas no mundo.

Conforme Saltiel (2025) a regularização dessa prática no Brasil, envolve o entendimento de uma das primeiras convenções internacionais que tratou de crimes cibernético em escala global – Conveção de Budapeste do ano de 2001- editada para harmonizar as leis e facilitar a cooperação entre pais visando punir crimes cibernético vindo a ser promulgada no país com atraso, pois só ocorreu no ano de 2023 através do Decreto nº 11.491/23.

No âmbito interno, alguns esforços nesse sentido são as Leis Carolina Dieckmann (Lei 12.737/2012) que estabeleceu no art. 154-A do Código Penal, tipificando o crime de "Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização[...]". Ainda nesse sentido, a Lei Azeredo (Lei nº 12.735/12) também soma esforço nesse sentido, pois tipificou crimes cibernéticos com alteração do Código Penal, obrigou a retirada de conteúdos racistas com alteração da Lei de Combate ao racismo (Brasil, 2012).

Logo em seguida, conforme já mencionado nesse estudo, foi editado o Marco Civil da Internet (Lei 12.965/2014) considerado um marco em regulamentação de crimes digitais no Brasil, pois regula o uso da rede mundial de computadores e também declara princípios garantias, direitos e deveres no uso. Sob essa norma, é possível realizar de formada fundamentada a retira de conteúdos enganosos, como áudios, imagens e videoconferências falsificadas por técnicas de deepfakes. (Alves et al, 2024).

Até o ano de 2025, as plataformas somente eram responsabilizadas quando não realizavam a retirada de conteúdos após decisão judicial. No entanto, conforme entendimento recente do Supremo Tribunal Federal, por meio do Recurso Extraordinário (RE) 1037396, decidiu que "nas investigação de crimes contra a honra, os provedores s provedores só podem ser responsabilizados com indenização por exemplo, se descumprirem uma ordem judicial para a remoção do conteúdo" (Supremo Tribunal Federal, 2025). No entanto, segundo a Suprema Corte, as plataformas podem devem remover publicações com base apenas em notificação extrajudicial.

No caso de crimes em geral, conforme o Pretório Excelso, enquanto o Congresso não editar nova lei sobre esse tema, as plataformas podem ser responsabilizadas civilmente pelos danos decorrentes de conteúdos gerados por terceiros em casos de crimes em geral ou atos ilícitos.

Outra norma que merece destaque no combate às falsificações no meio digital é a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018) que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade[...]" (Brasil, 2018).

As condutas perpetradas podem ser responsabilizadas de outras formas, a depender do contexto, como calúnia, injúria e difamação quando for utilizado para manchar a reputação de alguém ou como estelionato eletrônico por exemplo, quando for utilizado para obter vantagem financeira indevida por meio digitais. Além do crime de falsidade ideológica quando utilizado para enganar ou fraudar (Almeida, 2024).

Apesar do contexto normativo apresentado, evidencia-se que ainda não há um tipo penal específico para deepfakes no Brasil, o que cria brechas para que os responsáveis por atos maliciosos por vídeos e imagens falsos não sejam punidos com o rigor da Lei.

5.2 DESAFIOS PARA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Nesse cenário de acordo com Ruiz (2025) as falsificações por uso de deepfakes traz desafios para aplicação da LGPD, que é considerada atualmente, o principal instrumento infralegal de regulamentação do tema, pois expressa princípios e assegura direitos fundamentais aos indivíduos. Nesse sentido, a LGPD consolida o compromisso do País em criar um ambiente digital seguro e ético, trazendo meios para responsabilização dos agentes e alinha o Brasil às tendências globais de valorização da privacidade.

Segundo Mendonça e Rodrigues (2024) esse é um problema novo, que carece de regulamentação mais aprofundada, indo além das diretrizes criadas pela LGPD, exigindo tanto da doutrina como da sociedade civil, um debate mais aprofundado sobre educação digital, desinformação e circulação de imagens falsas.

5.3 REFLEXÕES ÉTICAS: MANIPULAÇÃO DA VERDADE, EROSÃO DA CONFIANÇA SOCIAL E RISCOS À DEMOCRACIA

A evolução das deepfakes no contexto geral, é um capítulo inédito entre as sociedades e uso da tecnologia. Apesar da manipulação de imagens não ser um fenômeno novo, o uso de deepfakes e a manipulação realista do que seja verdade é um salto sem precedentes. Assim, esse ambiente de incerteza constante sobre a veracidade das informações em imagens, áudio e vídeo no meio digital,

pode resultar em um ceticismo extremo, onde as pessoas passam a duvidas até mesmo de evidências legítimas, comprometendo a base do discurso democrático.

Com isso, surge também um outro efeito danoso a longo prazo, o descrédito nas instituições democráticas e da própria mídia. Assim, a partir do momento em que não é possível diferenciar o que é verdadeiro do que é falso, os direitos à dignidade, à honra, à informação, liberdade sexual entre outros direitos são afetados e colocam em risco o próprio Estado Democrático de Direito. Seja por afetar bens jurídicos em sua esfera particular como a honra ou no contexto coletivo como o interesse público em realidades políticas falsas por exemplo.

6 MECANISMOS DE DETECÇÃO, CONTROLE E PREVENÇÃO

Nesse capítulo apresenta-se as principais tecnologias empregadas no rastreamento e detecção de deepfakes, experiências internacionais com essa problemática, além de mecanismo para boas práticas jurídicas e institucionais de prevenção e correção.

6.1 TECNOLOGIAS EMERGENTES DE RASTREAMENTO E DETECÇÃO

A era da deepfakes introduz desafios para verificação da verdade, onde a rapidez e a precisão são cruciais para isso. Portanto, além da falta de regulamentação específica para combater as práticas criminosas por deepfakes, há também o desafio de criar mecanismos seguros para identificação e distinção do que é real e enganoso no meio digital. Esse cenário torna-se ainda mais gravoso com a existência do fenômeno "*liar's dividend* ou "*Dividendo do mentiso*" que se traduz em uma situação paradoxal onde a mera existência de *deepfake* cria um ambiente de desconfiança geral, o que possibilitam que pessoas mal intencionadas desacreditem conteúdos autênticos, o que prejudica as instituições e o próprio Estado Democrático (Tavares, 2024).

Nesse sentido, no enfrentamento desse desafio de detecção, é fulcral o desenvolvimento de abordagem multifacetada. Incluindo o avanço das tecnologias de detecção de *deepfakes*, a implementação de sistemas de verificação mais robustos e ágeis, e um esforço concertado de educação midiática para o público em geral. Ademais, exige-se protocolos claros e confiáveis para a autenticação de conteúdo, possivelmente utilizando tecnologias emergentes como *blockchain* que facilitando as transações por agrupá-las em blocos encadeados e compartilhadas entre os participantes de uma rede, não podendo os dados ser alterados sem consentimento da maioria (Diudice et al, 2021).

Atualmente diversas abordagens têm sido propostas para detecção de deepfakes, sendo a ciência forense uma das aliadas, como por exemplo o exame de vídeos adulterados para encontrar inconsistências , como o piscar dos olhos; como a pessoa do vídeo fala, analisando se o áudio e o movimento da boca se encaixam; a pele da pessoa do vídeo ou foto; o uso de óculos também é um

grande aliado, visto que pode ser analisado o ângulo e a iluminação do mesmo; os pelos faciais e o tamanho e cor dos lábios também são pontos importantes para análise (Ezeakunne e Liu 2024).

Portanto, as principais propostas de detecção de deepfakes são agrupadas, principalmente, em três categorias, as inconsistências físicas, abordagens orientadas por dados e técnicas que são focadas em artefatos de sínteses. No caso das inconsistências físicas, há discrepâncias fisiológicas, que mesmo sutis são perceptíveis a olho nu. Já as abordagens orientadas por dados, utilizam redes neurais profundas e redes de memória de curto e longo prazo, que são treinadas com grande volume de dados reais e sintético conforme diversidade demográfica, favorecendo modelo diante diversos perfis populacionais. Na detecção por artefatos, percebe-se que a geração de conteúdos sintéticos introduz distorções, desfoque e padrões anômalos que são explorados por método de detecção (Diudice et al, 2021).

Diante desse contexto, saliente-se que o desafio para verificação das informações não é meramente tecnológico, sendo também epistemológico, sendo exigível de todas a noção de verdade e evidências em meio às novas tecnologias.

6.2 EXPERIÊNCIAS INTERNACIONAIS E INICIATIVAS REGULATÓRIAS

Diante o aumento de casos e da gravidade do mal uso das deepfakes, conforme Teixeira (2024) há em andamento uma iniciativa da OpenIA que criou o ChatGPT,e outras criadoras de conteúdos que possibilitam o uso de deepfakes, como Intel, Sony, Google, Microsoft, adobe entre outras, em realização a junção dessas empresas para somar esforços conjuntos em fornecer técnicas e táticas que possam rastrear a origem e autenticidade dos conteúdos gerados por Inteligência Artificial, utilizando seus próprios metadados que ficam escondidos nos conteúdos gerados.

No mundo todo há esforços em regular essa tecnologia, por exemplo na China, o governo introduziu normas que obrigam as pessoas e instituições divulgarem quando utilizam a tecnologia deepfake em mídias digitais. Seguindo esse entendimento, o Canadá apresenta estratégia tripla de enfrentamento, incluindo prevenção deteção e resposta. Assim, aquele país trabalha também a conscientização do público sobre a tecnologia enquanto desenvolve sistemas de detecção. Indo de encontro às respostas desses outros países, a União Europeia tem aumento o número de pesquisas sobre a deteção e prevenção, bem como elaborado regulamentações que exigem rotulagem clara de conteúdos gerados artificialmente (Lawson, 2023).

6.3 MECANISMOS PREVENTIVOS E CORRETIVOS NO BRASIL

No Brasil as medidas de prevenção e correção das deepfakes, ainda são muito tímidas. Recentemente o Supremo Tribunal Federal lançou um programa de combate à desinformação, que

possui como eixos a compreensão a desinformação, reduzir os impactos das notícias fraudulentas, recuperar a confiança das pessoas (Filho, Marrafon e Medón, 2022).

Como ainda não há regulamentação especifica do combate as deepfakes, já no ano de 2025 o Senado Federal aprovou projeto de Lei (PL 370/2024) que eleva a pena de dois anos e multa, aumentada da metade, para o crime de violência psicológica contra mulher, que seja cometido por meio de manipulação da imagens e vídeos.

Portanto, as iniciativas tímidas, prejudicam o combate a esse tipo de desinformação, necessitando de maiores esforços para regulamentação específica e abrangente do uso dessa tecnologia. Quando somado a um maior empenho governamental na alfabetização digital das pessoas e maior empenho das plataformas, afastando-se da omissão de assumir políticas de responsabilidade, pode render bons frutos de enfrentamento aos deepfakes.

6.4 PROPOSTAS DE BOAS PRÁTICAS JURÍDICAS E INSTITUCIONAIS

Diante a ameaça por deepfakes no cenário brasileiro atual, exige-se uma resposta multidimensional, integrada e multidisciplinar, ou seja, uma abordagem holística e com a participação de aspectos tecnológicos, legais, colaborativos e educacionais. Assim, a boa prática para combate, passa pelo desenvolvimento de ferramentas capazes de detectar, exigindo um arcabouço jurídico específico para punibilidade dos crimes perpetrados (Tavares, 2024).

Nesse sentido, o desenvolvimento de ferramentas de análise forenses específicas para identificação de conteúdo produzidos por deepfakes, proporcionam a facilitação da produção probatória, que somada a alfabetização digital e a conscientização sobre os riscos associados ao uso de deepfakes, possibilita às pessoas possam discernir entre o real e o fabricado, no contexto de mundo digital. Portanto, o alinhamento entre instituições educacionais, governos e organizações da sociedade civil desempenha um papel fulcral na promoção da educação e na construção de uma sociedade mais capaz de enfrentar os desafios das deepfakes (Cyrineu, 2024).

Indo ao encontro desse somatório de esforço conjunto, a colaboração internacional é capaz de somar como elemento estratégico essencial nesse contexto. Sendo imperioso a formulação de parcerias com governos e organismos internacionais que estejam lidando com esse fenômeno, ampliando o repertório de estratégias disponíveis.

7 CONSIDERAÇÕES FINAIS

Diante o objetivo de analisar como a disseminação de deepfakes compromete a integridade das informações e impacta os direitos fundamentais. Concluir-se que o uso dessa tecnologia, apesar do seu uso benéfico em determinados meios quando aplicada com criatividade ética e responsável, representa

um enorme desafio na proteção das informações, sendo um ameaça real ao próprio processo democrático, uma vez que tem o poder de desacreditar as pessoas e as próprias instituições.

Soma-se a isso, que essa tecnologia compromete direitos fundamentais essenciais, tais como o direito à privacidade, honra, imagem e liberdade de expressão, dificultado o seu combate, pois requer bastante moderação das instituições ante a inexistência de acabou legal que tipifique essas condutas, sendo tais ações criminosas enquadradas conforme o resultados produzido, como calúnia, injúria e difamação, estelionato eletrônico, e/ou mesmo o uso da Lei Geral de Proteção de dados – LGPD, muito utilizada para fundamentar a remoção de conteúdos da internet.

Por fim, observa-se que, tais desafios são também oportunidades para fortalecimento das instituições no Brasil, devendo estas, buscarem os acertos legislativos de outras nações que lidam com essa mesma problemática, optando pelo fortalecimento multidisciplinar e integral que envolve avanços tecnológicos, educacionais e jurídicos.

REFERÊNCIAS

AFFONSO, Filipe José Medon. **O direito à imagem na era das deepfakes**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 27, p. 251-277, jan./mar. 2021.

ALMEIDA, F. C. **Deepfake: tecnologia permite colocar rosto e voz em outro corpo**. Jul. 2020. Disponível em: https://vejasp.abril.com.br/cultura-lazer/deepfake-tecnologia-permite-copiar-o-rosto-expressao-e-a-voz/. Acesso em: 15 out 2025.

ALVES, B. M., *et al.*. **Análise da responsabilização criminal dos criadores e propagadores de "deep fakes" no ordenamento jurídico brasileiro**. **Caderno Pedagógico,** *[S. l.]*, v. 21, n. 6, p. e4348 , 2024. DOI: 10.54033/cadpedv21n6-075. Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348. Acesso em: 11 out 2025.

ÁVILA, G. N.; CORAZZA, T. A. M. . **A Hiperexposição pessoal e seus reflexos nos direitos da personalidade**: necessidade de uma tutela transversal do direito à privacidade, com enfoque no âmbito penal. Juris Poiesis, v. 25, p. 144-177, 2022. https://mestradoedoutoradoestacio.periodicoscientificos.com.br/index.php/jurispoiesis/article/view/10540. Acesso em: 24 set 2025.

BESCHIZZA, Rob. R**owan atkinson deepfaked into the j'adore** ad. Boing Boing, 12 dez. 2019. Disponível em: < https://boingboing.net/2019/12/12/rowan-atkinson-deepfakedinto.html>. Data de acesso: 18 set 2025.

BRASIL, D. R.; Bento, L. A. **O direito fundamental à privacidade no contexto da Lei Geral de Proteção de Dados**. 2023. Revista De Direito Contemporâneo UNIDEP, 1(2), 7–24. Recuperado de https://periodicos.unidep.edu.br/rdc-u/article/view/162. Acesso em: 20 set 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15 set 2025.

BRASIL. **Lei Geral de Proteção de Dados**. (Lei nº 13.709/2018). Disponível em: Acesso em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 out 2025.

CARVALHO, Luiz Alberto David. **Liberdade de Expressão e as Fake News no Contexto Digital**. Revista de Direito Constitucional, 2022.

CHAGAS, Fernando Cerqueira; MORAES, Guilherme Peña de. "**Fake News no Direito Eleitoral".** In: Revista Justiça Eleitoral em Debate, volume 13, número 2, 2023, p. 31-39 (ISSN 2317-7144). Disponível em https://revista.tre-rj.jus.br/rjed/article/view/185. Acesso em: 23 set 2025.

CYRINEU Rodrigo Terra; MELÓN, Renato. **"IA e deep fakes nas eleições: desafio da tecnologia à integridade eleitoral (parte 2)".** *Conjur* 29 de abril de 2024. Disponível em: <https://www.conjur.com.br/2024-abr-29/ia-e-deep-fakes-nas-eleicoes-desafio-da-tecnologia-a-integridade-eleitoral-parte-2/>. Acesso em: 15 out 2025.

DOFFMAN, Zak. **Aplicativo chinês que coloca rosto em vídeos deixa milhões em risco.** *In:*Forbes, 03 set. 2019. Disponível em: <https://forbes.com.br/colunas/2019/09/aplicativochines-de-que-coloca-rosto-em-videos-poe-milhoes-em-risco/>. Acesso em: 14 out 2025.

EZEAKUNNE, U., Eze, C., e LIU, X. **Data-driven fairness generalization for deepfake detection.** In Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP). To appear. 2024. Disponível em: https://arxiv.org/abs/2412.16428. Acesso em: 12 out 2025.

FIGUEIRA, J., SANTOS, S. **As Fake News e a Nova Ordem (Des)Informativa na era da Pós-Verdade.** Coimbra: Imprensa da Universidade de Coimbra, 2020, ISBN: 978-989-26-1777-0.

FILHO, I.N.R.; MARRAFON, M.A.; MEDÓN, F. **A Inteligência Artificial a Serviço da Desinformação:** como as Deepfakes e as Redes Automatizadas Abalam a Liberdade de Ideias no Debate Público e a Democracia Constitucional e Deliberativa. Economic Analysis of Law Review, Brasilia, v. 13, n. 3, p. 32-47, Out 2022. Disponível em: https://www.proquest.com/docview/2841146127/fulltextPDF/8C87EDA36C504E3APQ/1?accountid=8112&sourcetype=Scholarly%20Journals. Acesso em: 22 set 2025.

GIUDICE, O., GUARNERA, L., e BATTIATO, S. **Fighting deepfakes by detecting GANDCT anomalies.** Journal of Imaging, 7(8). 2021. Disponível em: https://arxiv.org/abs/2101.09781. Acesso em 14 out 2025.

HASHIOKA, A, B. SILVA, A, Beatriz. MARCHETTO, P, Borba. **O uso do Deep Fake e a violação às garantias do estado democrático de direito. Rev. Humanidades e Tecnologias (FINOM).** ISSN 1809-1628**.** Disponível em: https://revistas.icesp.br/index.php/FINOM_Humanidade_Tecnologia/article/view/6362. Acesso em: 20 set 2025.

LAWSON, Amanda. **Uma análise das abordagens globais de regulamentação do deepfake.** Disponível em: https://www.responsible.ai/a-look-at-global-deepfake-regulation-approaches/. Acesso em: 14 out 2025.

MARTÍNEZ, O, Navarro, et al. **Possíveis benefícios e riscos à saúde de vídeos deepfake:** um estudo qualitativo em estudantes de enfermagem. Enfermeiros. Rep. 2024 , *14* (4), 2746-2757. Disponível em: https://www.mdpi.com/2039-4403/14/4/203. Acesso em: 15 out 2025.

MENDONÇA, Helena C. F. Coelho; RODRIGUES, Paula Marques. **Deepfakenews e sua influência no universo feminino**. Migalhas, 4 jul. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI282987,31047Deep+fake+news+e+sua+influencia+no+univers o+feminino>. Acesso em: 14 out 2025.

MIYASHIRO, Kelly. **De Bonner a Pedro Bial: os famosos que viraram vítimas de nova deep fake.** Revista Veja. 2024. Disponível em: https://veja.abril.com.br/coluna/tela-plana/de-bonner-a-pedro-bial-os-famosos-que-viraram-vitimas-de-nova-deep-fake/. Acesso em: 15 out 2025.

NOVELLO, Roger, M, do Nascimento. **Manipulação do meio digital pelo uso do *deepfake*: impactos nos direitos da personalidade, regulamentação e a reparação de danos no âmbito da responsabilidade civil.** Rio de Janeiro, 2023. Disponível em: https://pantheon.ufrj.br/handle/11422/24618. Acesso em: 20 set 2025.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha. **Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital**. 2023. v. 19, p. 1-19. Rev. Eletrôn. Curso Direito UFSM. Santa Maria, 2024.

RUIZ, Matheus Cordeiro. O direito fundamental à proteção de dados pessoais no Brasil: desafios e perspectivas para a efetivação da LGPD. Revista Fórum de Teses, Rio de Janeiro, v. 29, n.146, 23

mai. 2025. Disponível em: https://revistaft.com.br/o-direito-fundamental-aprotecao-de-dados-pessoais-no-brasil-desafios-e-perspectivas-para-a-efetivacao-da-lgpd/. Acesso em: 14 out 2025.

SALTIEL, R, Gomes Von. **Os crimes cibernéticos no Brasil à luz da Convenção de Budapeste.** Consultor Jurídico. Disponível em: https://www.conjur.com.br/2025-jul-06/os-crimes-ciberneticos-no-brasil-a-luz-da-convencao-de-budapeste/. Acesso em: 15 out 2025.

SARMENTO, Daniel. **Liberdade de Expressão e Seus Limites no Direito Constitucional Brasileiro**. Revista de Direito Constitucional, 2020.

SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. **Deepfakes:** regulação e responsabilidade civil. O direito civil na era da inteligência artificial. 1 ed. São Paulo: Thomson Reuters, 2020.

SECURITY REPORT. Relatório anual Sumsub Identity Fraud Report 2023. **Deepfakes crescem 830% em um ano no Brasil, aponta relatório.** Disponível em: https://securityleaders.com.br/deepfakes-crescem-830-em-um-ano-no-brasil-aponta-relatorio/. Acesso em: 14 out 2025.

STRECK, Lenio Luiz; CATTONI DE OLIVEIRA, Marcelo Andrade. **Pode se, em nome da democracia, propor a sua extinção?**. Consultor Jurídico, 22 jun. 2020. Disponível em: https://www.conjur.com.br/2020-jun-22/streckcattoni-nome-democracia-Propor-extincao. Acesso em: 15 out 2025.

STRECK, Lênio. **Fake News e o Direito Constitucional à Informação**. Revista Brasileira de Direito, 2021.

SUPREMO TRIBUNAL FEDERAL. **Programa de Combate à desinformação.** Disponível em: https://portal.stf.jus.br/hotsites/desinformacao/. Acesso em: 14 out 2025.

SUPREMO TRIBUNAL FEDERAL. **STF define restrições para responsabilização de plataformas por conteúdo de terceiros.** Recurso Extraordinário (RE) 1037396. 2025. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/. Acesso em 14 out 2025.

TARTUCE, Flávio. **Direito civil: lei de introdução e parte geral.** 15. ed. Rio de Janeiro:Forense, 2019. v. 1. p. 264-315.

TAVARES C, de Mello. **Inteligência Artificial e deepfakes:** Desafios Jurídicos e Tecnológicos para Integridade do Processo Democrático e as Implicações para as eleições municipais de 2024.

TEIXEIRA, Pedro. **Criado do ChatGPT traça plano contra deepfake nas eleições em meio a falta de regulação.** Folha de São Paulo, 2024. Disponível em: https://www1.folha.uol.com.br/poder/2024/01/criadora-do-chatgpt-traca-plano-contra-deepfake-nas-eleicoes-em-meio-a-falta-de-regulacao.shtml. Acesso em: 15 out 2025.

VENTURA, Deisy. **Pandemia, Fake News e Liberdade de Expressão no Brasil**. Cadernos de Saúde Pública, 2020.