**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO
PAULO – CAMPUS BRAGANÇA PAULISTA
BRAGANTEC – FEIRA DE CIÊNCIA E TECNOLOGIA**

LAURA MARTINS VALENTIM

THEO SOUTO CARDOSO

MIRELLA NOVAIS OLIVEIRA (ORIENTADORA)

TALITA DE PAULA CYPRIANO DE SOUZA (COORIENTADORA)

DEEPPFAKES:

RISCOS, PREVENÇÃO E PROTEÇÃO NA IA

**BRAGANÇA PAULISTA
2024**

DEEPPAKES:
RISCOS, PREVENÇÃO E PROTEÇÃO NA IA

IFSP – CAMPUS BRAGANÇA PAULISTA
AV. MAJ. FERNANDO VALLE, 2013 - SÃO MIGUEL, BRAGANÇA
PAULISTA - SP, 12903-000

LAURA MARTINS VALENTIM
THEO SOUTO CARDOSO
MIRELLA NOVAIS OLIVEIRA (ORIENTADORA)
TALITA DE PAULA CYPRIANO DE SOUZA (COORIENTADORA)

2024

DEDICATÓRIA

Nós dedicamos este trabalho aos nossos pais e mães. Esta pesquisa também é dedicada e direcionada a todas as pessoas que sofreram por causa de *deepfakes* e tiveram sua reputação prejudicada.

AGRADECIMENTO

Agradecemos as nossas professoras: Prof. Mirella Novais Oliveira e Prof. Talita Cypriano, que foram nossas orientadoras neste trabalho, desempenhando tal função com dedicação e amizade.

LISTA DE FIGURAS

FIGURA 1 – INSTRUÇÕES PARA IDENTIFICAR VÍDEO DEEPFAKE	17
FIGURA 2 – PROCEDIMENTOS DE SEGURANÇA	17
FIGURA 3 – INDICADORES TEXTUAIS E ANOMALIAS	18
FIGURA 4 – SOFTWARE DE DETECÇÃO DE DEEPFAKE	19
FIGURA 5 – INSTRUÇÕES DE DENÚNCIA NO FACEBOOK	20
FIGURA 6 – INSTRUÇÕES DE DENÚNCIA NO GOV.BR PARTE 1	21
FIGURA 7 – INSTRUÇÕES DE DENÚNCIA NO GOV.BR PARTE 2	22

SUMÁRIO

	RESUMO	7
1	INTRODUÇÃO	8
2	OBJETIVOS	9
3	RELEVÂNCIA	10
4	DESENVOLVIMENTO	11
4.1	RISCOS	11
4.2	PREVENÇÃO	13
4.3	PROTEÇÃO	20
5	RESULTADOS	27
6	CONCLUSÃO	28
	REFERÊNCIAS BIBLIOGRÁFICAS	29

Este projeto de pesquisa investiga os desafios apresentados pelas *deepfakes*, vídeos e áudios falsificados por Inteligência Artificial (IA), que representam sérios riscos à privacidade e à autenticidade das informações. Assim sendo, é finalidade deste trabalho apresentar recursos e legislação de uso nacional de prevenção e proteção contra as *deepfakes*, fundamentados nas ideias de autores como Chesney e Citron (2019), que enfatizam a necessidade de políticas abrangentes para mitigar o uso malicioso da IA, considerando aspectos técnicos, éticos e legais. Nessa perspectiva, desenvolve-se alguns objetivos específicos a saber: conceituar *deepfakes* e os principais recursos tecnológicos utilizados para produzi-las; indicar os impactos das mesmas nos direitos à privacidade e à segurança; e descrever a Lei Geral de Proteção de Dados (LGPD), além de outros recursos de prevenção e proteção em vigência no Brasil contra as falsas informações criadas por Inteligência Artificial. Este estudo é crucial para compreender e minimizar os danos das *deepfakes* e da dublagem viva, especialmente em contextos como disseminação de *fake news*, difamação e desinformação. Isso, porque, apesar dos avanços na detecção, há lacunas significativas que exigem novas abordagens para melhorar a precisão dos métodos preventivos. Por fim, entende-se que conectando-se aos debates sobre ética tecnológica e regulação, este projeto contribui para o desenvolvimento de políticas que promovam o uso responsável da IA, visando proteger a privacidade, a integridade das informações e a autenticidade cultural na sociedade atual.

PALAVRAS-CHAVE: Deep fakes, Inteligência Artificial, proteção.

1 INTRODUÇÃO

O avanço das tecnologias de Inteligência Artificial (IA), especialmente as *deepfakes*, traz preocupações significativas sobre a privacidade e a autenticidade das informações e pessoas. Este estudo investiga os impactos delas, como nos proteger das mesmas e os riscos que representam para a sociedade. Para tal, fez-se imperativo conceituar tal termo como o processo pelo qual a inteligência artificial (IA) combina ou substitui áudios e imagens para criar arquivos falsos, no qual pessoas podem ser colocadas em situações fictícias, dizendo frases que nunca foram ditas ou adotando comportamentos que nunca tomaram. Ao considerar a terminologia como sendo a junção de dois termos estrangeiros, "deep" (profundo) e "fake" (falso), vale ainda frisar que a palavra "deep" indica a profundidade da técnica de aprendizado (deep learning) usada para realizar essa manipulação.

Diante dessas afirmações, chegou-se à hipótese de que essas tecnologias representam riscos para a privacidade e autenticidade, sendo crucial analisá-las e encontrar formas de prevenir-nos e proteger-nos das mesmas. Assim, a pesquisa explora como tais inverdades são criadas, os riscos envolvidos e quais medidas já existem para prevenir seu uso indevido. Sobre esse tema, autores como Chesney e Citron (2019) argumentam que políticas claras são necessárias para controlar o uso malicioso de IA, considerando aspectos técnicos, éticos e legais, caminhos e teorias que foram seguidas para o desenvolvimento desta investigação. Dessa forma, o estudo se conecta aos debates sobre o avanço da IA, ética tecnológica e a urgência de regulamentação para preservar a privacidade, considerando aspectos que já foram estudados anteriormente, ainda que sob outros objetivos e pretensões de resultados.

Por outro lado, a questão legal é um fator que permeia sempre o universo das falácias e criações falseadas do mundo virtual, valendo destacar que autores como Raul Bergesch (2024), ao discutirem a criminalização do uso

malicioso de IA, oferecem *insights* cruciais sobre as medidas legais necessárias. Assim, este projeto visa uma análise cuidadosa das *deepfakes*, explorando seus riscos e estratégias de proteção, para contribuir também com o debate sobre regulamentação na tecnologia, na busca por um uso responsável das Inteligências Artificiais, visando mitigar seus impactos negativos na sociedade. Outrossim, enfatiza-se aqui a urgência de enfrentar os desafios das *deepfakes* na atualidade, adquirindo conhecimento desde os perigos que elas apresentam, passando por ferramentas que induzam à segurança no ambiente virtual, até alcançar as esferas regulamentares vigentes e eficazes na responsabilização e punição dos transgressores.

2 OBJETIVOS

OBJETIVO GERAL:

Apresentar recursos e legislação de uso nacional de prevenção e proteção contra as *deepfakes*, sobretudo em recursos audiovisuais.

OBJETIVOS ESPECÍFICOS:

- 1) Conceituar *deepfakes* e os principais recursos tecnológicos utilizados para produzi-las, sobretudo em recursos audiovisuais;
- 2) Indicar os impactos das *deepfakes* nos direitos à privacidade e à segurança;
- 3) Descrever a Lei Geral de Proteção de Dados (LGPD) e outros recursos de prevenção e proteção em vigência no Brasil contra as *deepfakes*.

3 RELEVÂNCIA

A inteligência artificial (IA) surgiu na década de 1950 e tem sua origem praticamente confundida com o próprio advento do computador. Porém, registros levam a precisar o evento no verão de 1956, quando ocorreu a Dartmouth College Conference, que passou a ser considerada o marco inicial da IA. A partir de tal evento, o uso da Inteligência Artificial foi se desenvolvendo cada vez mais, o que aumentou as dificuldades do discernimento sobre a legitimidade de textos, vídeos e principalmente imagens.

Enquanto a ética da manipulação digital ainda é discutida, programas e aplicativos realizam *deeplearning* ('machine learning', subconjunto do aprendizado de máquina que usa uma grande quantidade de dados vindos das redes e interações humanas para autodesenvolvimento de uma inteligência artificial), trazendo em sua maioria consequências sociais significativas, como as deepfakes audiovisuais.

Desde o primeiro caso de *deepfake*, registrado em novembro de 2017 no Reddit, uma rede social de discussões temáticas, a necessidade de as pessoas conhecerem os perigos, formas de segurança e denúncia já se faziam necessários, apesar das consequências em grande escala ainda não serem conhecidas. Na época, usava-se o apelido de um usuário e o nome de um fórum dedicado ao uso de IAs para substituir o rosto de atrizes pornôs pelo de celebridades mulheres. Tão logo foi descoberto, o grupo foi banido do aplicativo no início de 2018 e um estudo realizado pela empresa holandesa Deeptrace, especializada em algoritmos para identificar deepfakes, revelou que a quantidade de vídeos de tal natureza quase dobrou em um ano, aumentando de 7.946 em dezembro de 2018 para 14.678 em dezembro de 2019.

As *deepfakes* visuais são produzidas por algoritmo, que usa inúmeras imagens e vídeos guardados no banco de dados para aprendizagem, permitindo a alteração de um vídeo ou foto com ajuda da tecnologia, podendo falsificar não apenas o presente como também o passado e até o futuro. Diante de tais evidências, é patente que este estudo é crucial para minimizar os danos causados pelas *deepfakes*, especialmente em situações como disseminação de *fake news* e difamação, que impactam negativamente no corpo social.

Apesar de muitos já entenderem como esses tipos de tecnologias são criados e seus potenciais usos prejudiciais, existem lacunas significativas devido ao rápido avanço tecnológico, exigindo o desenvolvimento de métodos mais eficazes de detecção e prevenção de forma contínua e atualizada a cada novo aspecto e aperfeiçoamento desses instrumentos de criação de conteúdo falso.

4 DESENVOLVIMENTO

4.1 RISCOS

Graças aos avanços nos sistemas, programas, aplicativos e demais ferramentas tecnológicas atuais, já vivemos em uma era na qual existe a possibilidade de criar informações audiovisuais extremamente convincentes aos olhos de um usuário com um mínimo de conhecimento de manipulação de imagens, o que caracteriza grande parte da população. Assim, álbis podem ser criados, inocentes podem ser culpabilizados de um crime, situações de natureza vexatória ou constrangedora podem ser expostas, sem que nenhuma delas tenha acontecido realmente fora do mundo virtual. Logo, este estudo buscará apresentar a seguir, alguns dos impactos das *deepfakes*, considerando os riscos que elas representam para a sociedade:

A) Privacidade e consentimento: O uso inadequado de dados pessoais é uma preocupação central. A coleta e utilização de dados sem um consentimento claro e informado pode levar a violações de privacidade e exploração dos usuários. Isso é particularmente problemático quando a

tecnologia é empregada para fins que os indivíduos não esperavam ou não aprovaram explicitamente.

B) Transparência e controle: A falta de clareza sobre como os dados são coletados e utilizados pode minar a confiança pública na tecnologia geram processos opacos e confusos, dificultando que os usuários compreendam ou controlem o uso de suas informações pessoais, o que pode levar a um sentimento de exploração e desamparo.

C) Impactos sociais e éticos: A implementação de IA sem considerar o impacto social e ético pode resultar em consequências prejudiciais, como decisões injustas e desigualdades. Nisso, os Sistemas de IA podem perpetuar preconceitos existentes ou criar novos problemas se não forem projetados e geridos com cuidado.

D) Autonomia e controle: A interação entre humanos e máquinas inteligentes levantam questões sobre quem realmente controla as decisões e as ações. A autonomia compartilhada entre humanos e sistemas de IA pode ser complexa, e o controle inadequado pode levar a resultados indesejados ou perigosos.

Na era da IA, a privacidade na Internet torna-se objeto de novos, emergentes e muito significativos riscos. Comparando o papel dessa rede na violação da privacidade e o papel semelhante da imprensa, podemos afirmar que ambos podem expor informações pessoais e sensíveis. No entanto, a escala e a profundidade dessas consequências mudam com o desenvolvimento tecnológico, como a maneira com as quais as informações são divulgadas, tornando dados pessoais acessíveis e compartilhados globalmente, a maior parte do tempo, sem o consentimento dos envolvidos.

A criação de *deepfakes* é facilitada por tecnologias avançadas, como redes neurais convolucionais (CNNs) para reconhecimento facial, *autoencoders* para mapeamento de atributos, processamento de linguagem natural (NLP) para gerar áudio sintético e o poder de computação fornecido por sistemas de computação de alto desempenho. Ferramentas como *Deep Art Effects*, *Deepswap* e *FaceApp* exemplificam a acessibilidade da geração de *deepfake*, apontando para um futuro em que a criação de *deepfakes* convincentes estará ao alcance de muitos.

Com a ajuda de algoritmos sofisticados, dados pessoais podem ser explorados de maneiras que não eram possíveis antes, levando à criação de perfis detalhados apenas com a base de atividades aparentemente inofensivas. Esses, por sua vez, podem ser usados para criar conteúdo manipulado ou para segmentar e direcionar campanhas publicitárias e políticas de maneira muito mais eficaz e invasiva.

A IA também piora a impunidade e a jurisdição, uma vez que a atividade pode ocorrer em países estrangeiros, nas quais as leis de privacidade são mais flexíveis ou inexistentes. Nesses casos, a aplicação dos direitos permanece um desafio e cria uma situação na qual *deepfakes* ou *fakenews* são mais difíceis de rastrear e punir. Portanto, a combinação da Internet com a IA não só amplia o alcance da exposição de dados pessoais, mas também complica a proteção desses dados, exigindo uma abordagem mais robusta e adaptada para enfrentar esses novos desafios.

Sobre essa temática, o site da E.SAFER, empresa voltada para serviços de gerenciamento no setor de cibersegurança e ameaças cibernéticas, localizada em São Paulo, afirma que “nos últimos anos, surgiram vários exemplos notáveis de *deepfakes* que geraram manchetes e acenderam o alerta sobre os perigos dessa tecnologia”. Um desses casos envolveu um vídeo falso do ex-presidente dos Estados Unidos, Barack Obama, em que ele parecia fazer um discurso controverso e ofensivo. Outro exemplo famoso é o uso dessa tecnologia para criar vídeos de celebridades em situações comprometedoras, ampliando a disseminação de informações falsas e difamação. Destaca-se ainda, o uso dessas ferramentas de falseamento audiovisual em redes sociais como o TikTok, no qual é muito fácil achar perfis dedicados a esses tipos de vídeo para recriar situações com celebridades e que acabam confundindo muitas pessoas, chegando até a manipular não somente a imagem mais também o áudio, imediatamente levantando preocupações sobre a autenticidade de discursos e entrevistas.

O papel da mídia diante da divulgação dos riscos também é um fator extremamente importante para atingir as massas. Recentemente, a novela "Travessia" teve uma de suas personagens baseada no caso de Fabiane Maria de Jesus, que foi espancada e morta por moradores de Guarujá, por

culpa de um boato gerado por uma página em uma rede social, na qual afirmava que ela sequestrava crianças para rituais de magia negra. Em Travessia, a personagem Brisa tem seu rosto colocado sobre a imagem de uma mulher criminosa procurada pela polícia com a ajuda de inteligência artificial e sofre consequências devastadoras, ilustrando os riscos associados ao uso indevido de tecnologias de reconhecimento facial e à propagação de notícias falsa. Tal situação destaca como a tecnologia, quando mal utilizada, pode amplificar e perpetuar erros e injustiças, resultando em violência e sofrimento para indivíduos inocentes. Nesse sentido, a teledramaturgia serviu como um alerta sobre a necessidade de mecanismos rigorosos de verificação e regulamentação para evitar tais tragédias.

Tais exemplos destacam a facilidade com que essa tecnologia pode ser explorada para prejudicar a reputação de pessoas e disseminar informação. Nesse sentido, vale discutir a responsabilidade das empresas cibernéticas facilitadoras da criação de tais conteúdos e as implicações tanto econômicas, quanto sociais que envolve o sucesso alcançado pelas *deepfakes* entre seus usuários. É o caso, por exemplo da Meta, que enfrenta críticas por sua abordagem ao usar o conteúdo do Instagram para treinar seus modelos de IA. Essa empresa tem sido acusada de violar a privacidade dos usuários ao coletar e utilizar suas imagens e vídeos sem um consentimento claro e acessível.

A dificuldade para os usuários optarem por não participar de abordagens dessa natureza, evidenciada por um processo complexo e confuso, reflete uma falta de transparência e respeito pelos direitos dos indivíduos. Essa prática destaca os riscos de exploração e desamparo associados à IA, além de levantar questões sobre o controle e a responsabilidade na utilização de dados pessoais. A situação da Meta exemplifica como a tecnologia pode ser usada de forma a beneficiar as empresas às custas dos direitos e da privacidade dos usuários, ressaltando a necessidade urgente de regulamentações e práticas éticas na aplicação da mesma para impedir consequências futuras negativas.

4.2 PREVENÇÃO

Uma vez apresentados os riscos no uso das IAs para manipulação de imagem e voz em áudio e vídeo sem autorização, faz-se essencial que sejam elencados alguns métodos preventivos. Entretanto, cabe ressaltar a necessidade de que esses recursos sejam desenvolvidos e atualizados constantemente de uma forma bem mais robusta para mitigar os riscos associados a essa tecnologia. Assim deve ser, devido ao fato de que mesmo com a presença de alguns artifícios de vigília cibernética no país, eles ainda se fazem insuficientes para que haja uma segurança total da integridade e privacidade dos que podem ser futuramente afetados.

Deepfakes utilizam redes neurais para manipular e gerar conteúdos que podem ser extremamente realistas, tornando-se uma ferramenta poderosa, mas potencialmente perigosa. As principais técnicas de criação de *deepfake* incluem:

A) Vídeo de origem: Utiliza um codificador automático com um codificador para analisar atributos e um decodificador para aplicar esses atributos ao vídeo de destino.

B) Áudio: Emprega GANs para clonar padrões vocais, permitindo a criação de réplicas de voz realistas.

C) Sincronização labial: Combina gravações de voz com vídeo, aumentando a ilusão de que o sujeito está falando as palavras gravadas, com o suporte adicional de redes neurais recorrentes para maior realismo. Com um uso mal-intencionado, essas tecnologias podem resultar em violação de direitos fundamentais, como a honra, a imagem e a privacidade. Por esse motivo, cabe destacar alguns métodos de prevenção alternativas.

Em um ambiente onde a IA e as *deepfakes* podem ser facilmente utilizadas para desinformação e manipulação, é crucial estabelecer uma estrutura legal que proteja os indivíduos. A Lei Geral de Proteção de Dados (2018) é um exemplo de legislação que busca regular o tratamento de dados pessoais, garantindo a boa-fé e a transparência nas atividades de tratamento. O artigo 6º da citada lei estipula princípios fundamentais, como a finalidade, a adequação e a segurança, que devem ser observados em qualquer tratamento de dados, incluindo aqueles usados para alimentar

algoritmos de IA.

A prevenção do uso de *deepfakes* para fins maliciosos deve começar com a adoção de medidas que promovam a transparência e a responsabilidade. O inciso VII do artigo 6º da LGPD destaca a necessidade de medidas técnicas e administrativas que protejam os dados pessoais contra acessos não autorizados. Isso é especialmente relevante no contexto das *deepfakes*, nas quais a manipulação de dados pessoais sem consentimento pode causar danos irreparáveis aos indivíduos.

Além disso, a Lei Geral de Proteção de Dados também aborda a questão da responsabilização e prestação de contas, que são essenciais para que os agentes de tratamento demonstrem a eficácia das medidas de proteção implementadas. O artigo 6º, inciso X, exige que "o agente comprove a observância e o cumprimento das normas de proteção de dados pessoais" (BRASIL, 2018).

Ainda se tratando das questões legais, cabe evidenciar o descrito no texto da Constituição Federal (1988):

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;

XII — é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Nesse trecho, garante-se a inviolabilidade da intimidade e do sigilo, sobretudo em caso de dano moral, características comuns quando se pratica a manipulação de imagem/áudio sem o consentimento do verdadeiro autor(a) e com claro objetivo de prejudicá-lo(a). Diante dessa problemática vale destacar ainda outros aspectos da legislação brasileira coadunados com esse tema:

A) Art. 9º da LGPD (2018): Este artigo dá ao titular (a pessoa cujos dados estão sendo tratados) o direito de acessar facilmente informações sobre como seus dados estão sendo usados. Se o consentimento for pedido, mas as informações forem enganosas ou não claras, esse consentimento não

vale. Se houver mudança na forma como os dados serão usados, a pessoa deve ser avisada e pode revogar o consentimento. Também deve ser informado se o uso dos dados é necessário para fornecer um produto ou serviço;

B) Art. 154-A do Código Penal (2022): Este artigo define o crime de invasão de dispositivos eletrônicos. Isso significa acessar computadores ou dispositivos sem permissão, podendo alterar ou apagar informações ou acessar dados privados para obter vantagens, causando prejuízo ao dono. As penas variam de 3 meses a 1 ano de prisão, e podem aumentar se houver prejuízo econômico. Se a invasão envolver comunicações privadas ou segredos comerciais, a pena é mais severa, de 6 meses a 2 anos de prisão, além de multa. A punição pode ser ainda maior se o crime for contra autoridades.

Para mitigar os riscos associados aos casos de *deepfakes*, é fundamental promover a educação digital e a conscientização sobre os direitos dos indivíduos em relação ao uso de suas informações. O artigo 9º da LGPD assegura que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados. Portanto, campanhas de conscientização podem empoderar os indivíduos, permitindo que eles compreendam seus direitos e como se proteger de abusos.

A tecnologia de *deepfakes*, embora inovadora, apresenta desafios significativos que exigem uma abordagem multidimensional, combinando regulamentação, responsabilidade corporativa e educação do público. O fortalecimento das normas existentes, como a LGPD, e a aplicação rigorosa de penalidades para práticas abusivas, como previsto no Código Penal Brasileiro, são fundamentais para garantir que a IA seja utilizada de maneira ética e responsável.

Além disso, as plataformas de mídia social, como *Facebook* e *Instagram*, devem ser transparentes sobre como utilizam dados para treinar modelos de IA, e os usuários devem ter a capacidade de se opor ao uso indevido de suas informações. Somente com um esforço conjunto será possível prevenir o uso de tecnologias de IA para a criação de *deepfakes* prejudiciais, protegendo assim os direitos humanos e promovendo um

ambiente digital mais seguro e ético.

Ademais, algumas empresas de segurança cibernética já atuam no campo da prevenção com o desenvolvimento de sistemas, programas e aplicativos com fins de criptografias e marcas digitais que dificultem ou identifiquem casos de *deepfakes*. Pode-se apresentar como exemplo as instruções contidas na página da *Kaspersky*, cujo site oferece algumas orientações a conhecer:

1) Um algoritmo criptográfico pode ser usado para inserir *hashes* em intervalos definidos durante o vídeo. Se o vídeo for alterado, os *hashes* serão alterados, assim a IA e *blockchain* podem registrar uma impressão digital à prova de adulteração para vídeos. Essa técnica é semelhante aos documentos de marca d'água. A dificuldade com o vídeo é que os *hashes* precisam se manter, caso o vídeo seja comprimido para uso com *codecs* diferentes;

2) Biometria multimodal – Envolve a combinação de vários métodos de autenticação biométrica para aumentar a segurança. Ao utilizar uma combinação de reconhecimento facial, reconhecimento de voz e biometria comportamental, por exemplo, é possível obter uma defesa mais robusta contra ameaças de *deepfake*.

Ainda no site da *Kaspersky* destacam-se algumas informações para identificação de vídeos criados com ajuda de IA, conforme indicado na figura a seguir:

FIGURA 1 – INSTRUÇÕES PARA IDENTIFICAR VÍDEO DEEPPFAKE

Os vídeos de deepfake ainda estão em uma fase em que você mesmo pode ser capaz de detectar sinais. Ao suspeitar de um vídeo de deepfake, procure pelas seguintes características:

- movimento brusco
- iluminação instável, mudando de um quadro para o outro
- mudanças no tom da pele
- modo de piscar os olhos estranho ou nenhum piscar
- lábios mal sincronizados com a fala
- elementos digitais na imagem

À medida que os deepfakes são aprimorados, o olho humano será cada vez menos eficaz, pre-
substituído por bons programas de segurança virtual.

Fonte: Site da Kaspersky

É importante destacar que os casos de *deepfake* continuam a evoluir. Há dois anos, era muito fácil identificar vídeos pela baixa qualidade dos movimentos e pelo fato de que a pessoa representada parecia nunca piscar os olhos. Mas a geração mais recente de vídeos falsos evoluiu e adaptou-se, inviabilizando o que já se conhece para identificar a farsa. Por isso, um estudo contínuo de estratégias preventivas devem ser estabelecidos e revisados a cada novo avanço tecnológico. Também é fundamental manter hábitos básicos de prevenção em redes domésticas e corporativas, como indicada na figura abaixo:

FIGURA 2 – PROCEDIMENTOS DE SEGURANÇA

Lembre-se de que, se o deepfake começar a ser implementado por hackers nas tentativas em redes domésticas e corporativas, as melhores práticas básicas de segurança virtual poderão desempenhar um papel fundamental quando se trata da minimização de riscos:

- Backups realizados com regularidade protegem os dados contra ransomware e oferecem a capacidade de restaurar dados danificados.
- Usar senhas diferentes e fortes para contas diferentes só porque uma rede foi invadida não significa que nenhuma outra conta tenha sido comprometida. Alguém invadir uma conta do Facebook, ninguém vai querer que essa pessoa invada outras contas também.
- Use um bom pacote de segurança, como o [Premium](#) da Kaspersky, para proteger computadores domésticos, laptops e smartphones contra ameaças virtuais. Esse pacote fornece software antivírus, rede VPN para impedir que as conexões Wi-Fi sejam invadidas e também protege as webcams.

Fonte: Site da Kaspersky

No site de outra empresa de segurança cibernética, *Malwarebytes*, é possível conferir ainda alguns indicadores textuais e anomalias comportamentais/contextuais que auxiliam na identificação de *deepfakes*, segundo imagem a seguir:

FIGURA 3 – INDICADORES TEXTUAIS E ANOMALIAS

Indicadores textuais:

- Erros de ortografia e frases gramaticalmente incorretas.
- Fluxo de frases que parece não ser natural.
- Endereços de e-mail que parecem suspeitos.
- Frases que não correspondem ao estilo esperado do remetente.
- Mensagens fora de contexto ou irrelevantes.

Além disso, considere as anomalias comportamentais e contextuais:

- **Inconsistências comportamentais:** Preste atenção ao comportamento e aos maneirismos. Os deepfakes podem não reproduzir com precisão traços sutis de personalidade, movimentos habituais ou respostas emocionais, fazendo com que o sujeito pareça um pouco estranho.
- **Anomalias contextuais:** Analise o contexto em que o vídeo ou áudio aparece. Discrepâncias de fundo, interações inesperadas com o ambiente ou anomalias no enredo podem indicar manipulação.

Fonte: Site da *Malwarebytes*

É imprescindível destacar ainda, que a luta contra as deepfakes também é apoiada pela inovação do setor privado. Várias empresas oferecem softwares sofisticados de detecção das ocorrências, fornecendo ferramentas essenciais para identificar mídias manipuladas, como as descritas no site da *Malwarebytes* e especificadas na figura seguinte:

FIGURA 4 – SOFTWARE DE DETECÇÃO DE DEEPPFAKE

- **Iniciativa de autenticidade de conteúdo da Adobe:** A Adobe introduziu um sistema que permite aos criadores anexar uma assinatura digital a seus vídeos e fotos. Essa assinatura inclui informações detalhadas sobre a criação da mídia, oferecendo um método transparente para verificar a autenticidade.
- **Ferramenta de detecção da Microsoft:** A Microsoft desenvolveu uma ferramenta com tecnologia que analisa vídeos e fotos para avaliar sua autenticidade. Ela fornece uma pontuação de confiança que indica a probabilidade de manipulação, ajudando os usuários a discernir a confiabilidade que encontram.
- **Operação Minerva:** Essa iniciativa se concentra na catalogação de deepfakes conhecidas e impressões digitais. Ao comparar novos vídeos com esse catálogo, é possível identificar novas falsificações descobertas anteriormente, aprimorando o processo de detecção.
- **Plataforma de detecção da Sensity:** A Sensity oferece uma plataforma que emprega inteligência artificial profunda para detectar mídia deepfake, de forma análoga à maneira como as ferramentas *antimalware* identificam *vírus* e *malware*. Ela alerta os usuários por e-mail se eles encontram conteúdo deepfake, adicionando uma camada extra de proteção.

Fonte: Site da *Malwarebytes*

Sobre a necessidade de atualizações legais que atendam às demandas dos crimes de internet no Brasil, sancionou-se o Decreto nº 10.222, de 5 de fevereiro de 2020, no qual se desenvolvem Estratégias Nacionais de Segurança Cibernética (E-Ciber). Na parte II do documento, no que tangem ao primeiro bloco de eixos temáticos, revelam-se estratégias de

proteção e segurança, envolvendo: governança da segurança cibernética nacional; prevenção e mitigação de ameaças cibernéticas internacionais; e proteção estratégica.

Por fim, a verdadeira prevenção contra a criação de falsas informações visuais reside na empatia e na responsabilidade dos usuários da Inteligência Artificial. Sem um controlador que atue de forma ética, a tecnologia por si só não possui valores intrínsecos. Assim, é vital que cada indivíduo que interage com essas ferramentas desenvolva uma consciência crítica e empática em relação ao impacto de suas ações no mundo digital. A promoção de um uso responsável da IA, pautado na ética e na proteção dos direitos fundamentais, é o caminho para um futuro no qual a inovação não comprometa a dignidade humana.

4.3 PROTEÇÃO

Com o avanço das IAs e seus perigos notáveis, foi necessária a criação de leis no código penal contra práticas que podem prejudicar a reputação e a integridade dos indivíduos e entidades. Nesse escopo cabe destacar principalmente: a Lei 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecida como o Marco Civil da Internet; a Lei 13.709 de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados (LGPD); bem como alguns artigos cobertos pelo direito penal já vigente em todo o território nacional e fiscalizado pela Polícia Civil dos estados e a Polícia Federal nos casos que envolvem usuários de outros países.

No que diz respeito ao Marco Civil, Lemos (2024) esclarece que “graças ao Marco Civil da Internet existe um artigo na lei que obriga as plataformas a removerem imagens e vídeos ... divulgadas sem autorização.” Tal recurso legal foi importante para que as principais plataformas criassem canais de denúncias, que possibilitam rapidez na remoção da deepfake e, conseqüentemente, minimiza os danos que essa possa causar às vítimas.

Tanto no *Facebook* como no *Instagram* essa opção de denúncia está explícita em uma das abas de segurança da plataforma, conforme figura a seguir:

FIGURA 5 – INSTRUÇÕES DE DENÚNCIA NO FACEBOOK

Comece aqui

Se alguém ameaçar compartilhar informações que você deseja manter confidenciais, pedir que você envie dinheiro ou outra situação desse tipo, lembre-se de que você tem outras opções:

1. Documentar a publicação: talvez você precise de um registro da publicação caso decida tomar outras providências. Saiba como fazer uma [captura de tela](#).
2. Denunciar a situação às autoridades locais.
3. [Denunciar a situação ao Facebook](#). Compartilhar ou ameaçar compartilhar imagens íntimas vai contra os [Padrões da Comunidade](#). Se alguém estiver ameaçando compartilhar itens pessoais que você deseja manter em privado (por exemplo, mensagens, fotos, vídeos), pedindo que envie dinheiro ou que faça qualquer outra coisa com a qual você não se sinta à vontade, denuncie essa pessoa para nós.
4. [Bloquear a pessoa](#). Dependendo das suas configurações de privacidade, as pessoas no Facebook podem ver uma lista dos seus amigos do Facebook. Ao bloquear uma pessoa, ela não terá mais acesso à sua lista de amigos e não poderá iniciar conversas com você nem visualizar itens publicados no seu perfil.

Lembre-se: se alguém pedir que você compartilhe algo com o qual não se sinta confortável, você tem o direito de dizer "Não".

Fonte: Central de ajuda do Facebook.

Ainda nessa perspectiva, Luís (2018) afirma que tanto o *Twitter* como a plataforma de *chat Discord* já disponibilizam a possibilidade de banir publicações de natureza *fake* da *timeline* de seus usuários. O autor elucida ainda que “não só empresas podem combater a existência dos “deepfakes”, mas também o Estado”. No Brasil, assim como nos Estados Unidos onde a maioria dos casos tem ocorrido, nenhuma legislação contempla especificamente este novo fenômeno digital, mas tanto algumas leis civis como penais podem ajudar a coibi-lo, bastando que a informação de como fazê-lo chegue ao maior número de pessoas possível.

Acerca dessa observação, vale destacar que no site oficial do governo (gov.br), no espaço destinado à Secretaria de Comunicação Social, é possível encontrar instruções sobre como fazer uma denúncia nas redes sociais com ilustrações passo a passo. Tal esforço de divulgação está acessível aos sujeitos brasileiros e poderá ser utilizado como uma fonte fidedigna de apoio às vítimas desse ato criminoso. Por isso, é de suma importância que cada vez mais indivíduos conheçam e repassem os procedimentos em caso de ser alvo de ações delituosas do tipo. A seguir estão os dados contidos no site:

FIGURA 6 – INSTRUÇÕES DE DENÚNCIA NO GOV.BR PARTE 1

Fonte: Site gov.br

No endereço eletrônico, além das ilustrações, também há a descrição do que fazer em cada plataforma, conforme os seguintes comandos:

A) Para Facebook ou Instagram:

Passo 01: Clique nos três pontinhos que aparecem no canto direito da foto ou vídeo;

Passo 02: Clique em denunciar;

Passo 03: Clique em informação falsa e escolha o tema do conteúdo.

B) Para LinkedIn:

Passo 01: Clique nos três pontinhos que aparecem no canto superior direito;

Passo 02: Selecione a opção denunciar esta publicação;

Passo 03: Selecione desinformação, escolha o tema e clique em denuncie.

C) Para Whatsapp:

Passo 01: Abra a conversa com o usuário e escolha mais opções > mais > denunciar.

É possível denunciar um contato ou grupo.

Outras plataformas também são contempladas com as instruções de denúncias no site, de acordo ao que se demonstra na figura seguinte:

FIGURA 7 – INSTRUÇÕES DE DENÚNCIA NO GOV.BR PARTE 2

Fonte: Site gov.br

Assim como nos demais casos, para essas plataformas também há uma sequência de comandos explicativos, a conhecer:

A) Para *TIKTOK*

Passo 01: Toque em compartilhar no canto inferior direito;

Passo 02: Pressione relatar > informações incorretas;

Passo 03: Escolha o tema e pressione enviar.

B) Para *Youtube*

Passo 01: Clique no símbolo de compartilhar;

Passo 02: Role a tela para a lateral e clique em denunciar;

Passo 03: Selecione informação falsa, escolha o tema e clique em denunciar.

C) Para *Twitter*

Passo 01: Clique nos três pontinhos no canto superior direito do post;

Passo 02: Escolha a opção denunciar post;

Passo 03: Defina o tipo e conclua.

Ademais desses dados para denúncia, também é primordial considerar o Código Civil (2002), no qual entende-se que a manutenção do direito do cidadão afetado por tais incursões de Inteligência Artificial está prevista no seu Capítulo II do que trata dos Direitos da Personalidade. Nele, o artigo 20 diz que “a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade”. Logo, sanções em torno da manipulação indevida da

imagem e áudio de um indivíduo sem a sua devida autorização estaria amparada em mais um aspecto legal brasileiro.

Sobre a Lei Geral de Proteção de Dados, no seu Art. 308 está especificado que “adulterar arquivos de vídeo ou de áudio, mediante clonagem da voz, substituição de rosto, sincronização labial ou outra ferramenta de Inteligência Artificial, com a intenção de divulgar notícias falsas ou prejudicar pessoa física ou jurídica” está sujeito à pena de reclusão, de dois a quatro anos, e multa. Assim, sabendo a presença de artigos de proteção, é possível executar uma aplicação da justiça, realizando uma denúncia ou processo com os responsáveis pela difamação de tais informações que atingem a integridade de um elemento ou de entidades.

Infelizmente as leis contra *deepfake* no Brasil ainda são bastante falhas e insuficientes para lidar com a complexidade e a rápida evolução dessa tecnologia. Embora existam algumas iniciativas legislativas que buscam coibir o uso malicioso dessas ações, como a divulgação não autorizada de imagens ou vídeos alterados, a aplicação dessas normas enfrenta desafios significativos, como a identificação dos responsáveis e a dificuldade de comprovar a manipulação.

Primeiramente, a definição de “notícias falsas” pode ser vaga e sujeita a interpretações diversas, o que pode levar a dificuldades na aplicação da lei. Além disso, a identificação de quem está por trás da criação e disseminação do material audiovisual é um desafio, uma vez que essas tecnologias podem ser usadas de forma anônima, dificultando a responsabilização. Ainda assim, alguns procedimentos são essenciais no momento em que todas as alternativas de proteção falham e o cidadão torna-se vítima da *deepfake*. Nesse caso, é imprescindível conhecer todos os passos que devem ser seguidos.

Sobre essa problemática, Jung (2024) apresenta um protocolo a ser ministrado não apenas para oferecer mais proteção aos atingidos pelas falsa e desautorizadas manipulações de imagem e áudio, como também para que outros agentes possam multiplicar essa rede protetiva pelas redes sociais e demais espaços cibernéticos. Com base nas informações dadas pela autora foi possível estabelecer um quadro de orientações para vítimas de

deepfakes, a seguir:

QUADRO 1 – ORIENTAÇÕES EM CASO DE *DEPPFAKE*

AÇÕES	MÉTODO
1) Reúna informações	<ul style="list-style-type: none">• <u>Identifique o caso de deepfake:</u>• <u>Documente a prova.</u>
2) Denuncie o caso de <i>deepfake</i>	<ul style="list-style-type: none">• <u>Denuncie em Plataformas:</u>• <u>Denuncie às autoridades.</u>
3) Comunique-se com seus contatos	<ul style="list-style-type: none">• <u>Informe pessoas próximas;</u>• <u>Faça um pronunciamento público.</u>
4) Proteja sua segurança online	<ul style="list-style-type: none">• <u>Altere senhas;</u>• <u>Monitore sua reputação online.</u>
5) Busque apoio	<ul style="list-style-type: none">• <u>Busque suporte emocional;</u>• <u>Busque assessoria jurídica.</u>

Fonte: Jung (2024)

O item 1 do quadro sugere que o indivíduo deva acessar o vídeo ou áudio e confirmar se é realmente uma imagem sua ou sua voz que está sendo usada. Deverá observar ainda detalhes como a qualidade da imagem ou som, inconsistências na fala ou movimento, e se o contexto da situação parece real. Ademais, indica-se que a vítima deve salvar cópias do caso de *deepfake* e de qualquer outra informação relevante, como *links* para onde ele foi publicado, datas e horários, e capturas de tela de comentários ou mensagens relacionadas. Deverá ainda identificar quem está repassando o conteúdo, salvar números de telefones e nomes de usuários em redes sociais.

Com o item 2, espera-se que o sujeito utilize os mecanismos de denúncia disponíveis nas plataformas nas quais o caso de *deepfake* foi publicado, como *YouTube*, *Facebook*, *Twitter*, etc. seguindo as instruções específicas de cada uma delas para reportar conteúdo falso ou prejudicial (ver figuras 1 e 2). Além disso, Se o caso contiver conteúdo difamatório, ameaçador ou ilegal, o mesmo deve ser denunciado às autoridades competentes. No Brasil existem algumas unidades específicas para este fim, mas na falta dessas o Boletim de Ocorrência pode ser realizado em qualquer

delegacia, presencialmente. A consulta às unidades policiais especializadas mais próximas pode ser feita no seguinte endereço eletrônico: <https://new.safernet.org.br/content/delegacias-ciber Crimes>. No estado de São Paulo é possível ainda fazer o registro de um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica (<https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/> home).

Nas considerações do item 3, destaca-se a necessidade de que o sujeito avise amigos, familiares e colegas sobre a situação e peça para que não o compartilhem, explicando a situação e solicitando ajuda para identificar e remover outras cópias online. Em alguns cenários é preciso ainda que a pessoa considere fazer uma declaração pública nas suas redes sociais ou em um comunicado oficial, esclarecendo que o conteúdo é falso e fornecendo informações sobre como denunciá-lo.

Para evitar futuros ataques cibernéticos, o item 4 indica que é recomendável que o cidadão troque as senhas de suas contas de e-mail, redes sociais e outros serviços *online* como medida de precaução. Também recomenda-se que o mesmo utilize ferramentas de monitoramento *online* para acompanhar as menções do seu nome e identificar novas publicações de *deepfake* ou conteúdo relacionado.

A saúde do usuário atingido é mencionada no item 5, no qual recomenda-se que esse busque apoio de amigos, familiares, um terapeuta ou grupos de apoio *online* para lidar com o estresse e a ansiedade. Deve-se considerar ainda, buscar mais tranquilidade, consultando um advogado especializado em crimes cibernéticos para avaliar suas opções legais e buscar reparação pelos danos causados, de acordo com o que prevê a legislação atual.

Tanto as práticas de proteção envolvendo as leis e o código penal quanto às estratégias abordadas anteriormente são ainda pouco eficazes para uma defesa sofisticada contra as *deepfakes*, pois atualmente a tecnologia avança muito rapidamente, dificultando a detecção de manipulações complexas e de uma proteção total, a qual os vídeos e imagens poderiam ser provadas como artificiais e falsas, não ferindo assim, a integridade e moralidade de entidades e indivíduos. Entretanto, não se

deve invalidar os aspectos legais que já criminalizam a adulteração dos arquivos que visam prejudicar pessoas, uma vez que esses são passos importantes e auxiliam na criminalização de tais atos. Quanto maior for a informação, menores serão as ocorrências desses feitos e mais pessoas serão responsabilizadas e punidas. Esse deve ser um compromisso de todos: empresas, sociedade e Estado.

5 RESULTADOS

Os resultados deste trabalho sobre deepfakes demonstram a gravidade e o impacto crescente dessa tecnologia na sociedade atual. Foram evidenciados os riscos significativos para a privacidade, segurança e integridade das informações, principalmente no uso de deepfakes para manipulação audiovisual. A pesquisa destaca que, embora a tecnologia tenha evoluído rapidamente, os mecanismos de prevenção e detecção ainda possuem lacunas que precisam ser preenchidas com maior rigor e eficiência.

O estudo identificou que, além de ameaçar a reputação pessoal, os deepfakes representam um risco à disseminação de desinformação e fake news, o que pode ter consequências graves, como vimos em exemplos que geraram tragédias reais. As medidas preventivas incluem a necessidade de legislações mais robustas, como a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet, que já oferecem mecanismos para lidar com a manipulação de informações. No entanto, é evidente que essas normas precisam ser continuamente atualizadas para acompanhar o avanço da IA.

Além disso, os resultados apontam para a importância de educar o público sobre os perigos das deepfakes e fornecer orientações claras sobre como se proteger e denunciar conteúdos fraudulentos. Empresas de cibersegurança, como Kaspersky e Malwarebytes, já desenvolvem ferramentas que ajudam a identificar deepfakes, mas a pesquisa enfatiza que um esforço conjunto entre o setor privado, público e a sociedade é essencial para mitigar os impactos dessa tecnologia.

6 CONCLUSÃO

A pesquisa buscou explorar como informações falsas tecnológicas, de recursos audiovisuais são criadas, os riscos envolvidos e quais medidas já existem para prevenir seu uso indevido, considerando o que autores como Chesney e Citron (2019) argumentam sobre a necessidade das políticas claras serem necessárias para controlar o uso malicioso de IA, considerando aspectos técnicos, éticos e legais. Logo, este estudo torna-se crucial para minimizar os danos causados pelas *deepfakes*, especialmente em situações como disseminação de *fake news* e difamação, que impactam negativamente o corpo social no campo audiovisual. Apesar de entendermos como elas são criadas e seus potenciais usos prejudiciais, existem lacunas significativas devido ao rápido avanço tecnológico, exigindo o desenvolvimento de métodos mais eficazes de detecção e prevenção.

Portanto, este trabalho se conecta aos debates sobre o avanço da IA, ética tecnológica e a urgência de regulamentação para preservar a privacidade, cujos recursos de autores como Bergesch (2024), ao discutirem a criminalização do uso malicioso de IA, são oferecidos em forma de *insights* cruciais sobre as medidas legais necessárias.

Espera-se com esse projeto alertar sobre os riscos das *deepfakes*, além de promover alternativas de prevenção e proteção contra elas. Ademais, pretende-se evidenciar que, embora já exista legislação sobre o tema, ainda carece complementar e especificar situações e sanções que acompanhem o rápido desenvolvimento tecnológico das Inteligências Artificiais, em prol de um espaço de progresso com marcas mais positivas do que negativas nas relações interpessoais e na validação de informações.

Em outrossim, cogita-se trabalhar futuramente na catalogação de mecanismos tecnológicos, também produzidos por las, para auxiliar e complementar a garantia dos direitos cidadãos de isonomia, autonomia e equidade, evidenciando que também existem inúmeros aspetos benéficos no

avanço da tecnologia e que o mesmo não pode ser sempre encarado como ameaça ou influenciador maléfico aos direitos humanos.

REFERÊNCIAS

BERGESCH, Raul. **Deep Fake é crime? O que é e como se prevenir.** BERGESCH Advogados, publicado em março de 2024. Disponível em: <https://ber.adv.br/blog/deep-fake-e-crime-o-que-e-e-como-se-prevenir/>. Acesso em: set de 2024.

BRASIL. **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: ago 2024.

BRASIL, **Decreto nº 10.222**, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: set 2024.

BRASIL, **Lei nº 10.406** de 10 de janeiro de 2002. Código Civil Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em ago 2024.

BRASIL, **Lei 12.965** de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em set 2024.

BRASIL, **Lei 13.709** de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em jun 2024.

CITRON, Danielle Keats ; CHESNEY, Robert. **Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.** University of Virginia School of Law. Date Written: July 14, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954.. Acesso em: set de 2024.

JUNG, Juliana Débora. **Fizeram um deepfake meu, e agora?** (Art). Jusbrasil. Publicado em jul de 2024. Disponível em: <https://www.jusbrasil.com.br/artigos/fizeram-um-deepfake-meu-e-agora/2566114584>. Acesso em: set 2024.

KASPERSKY. **Empresa de segurança virtual (site).** Disponível em:

<https://www.kaspersky.com.br/resource-center/threats/protect-yourself-from-deep-fake>. Acesso em: out 2024

LEMOS, Ronaldo. **O que fazer se fizerem uma deepfake com você?** Artigo da Folha de São Paulo. Publicado em 6 de fevereiro de 2024. Disponível em: <https://itsrio.org/pt/artigos/o-que-fazer-se-fizerem-uma-deepfake-com-voce/>. Acesso em set. 2024.

LUIS, Leonardo. **O que fazer se eu virar vítima de pornografia falsa na internet?** Publicado em: 23 de fevereiro de 2018. Disponível em: em <https://www.uol.com.br/tilt/noticias/redacao/2018/02/23/vitimas-de-pornografia-falsa-no-brasil-podem-pedir-indenizacao.htm?cmpid=copiaecola>. Acesso em ago 2024.

MALWAREBYTES. **Produtos e soluções cibernéticos** (site). Disponível em: <https://www.malwarebytes.com/pt-br/cybersecurity/basics/deepfakes>. Acesso em: out de 2024.