UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

SANIELLY AUREA DE SOUZA MARTINS

DEEPFAKE E A VIOLAÇÃO AO DIREITO DA PERSONALIDADE: análise da percepção de pessoas na cidade de Juazeiro do Norte-CE

JUAZEIRO DO NORTE-CE
2024

SANIELLY AUREA DE SOUZA MARTINS

DEEPFAKE E A VIOLAÇÃO AO DIREITO DA PERSONALIDADE: análise da percepção de pessoas na cidade de Juazeiro do Norte-CE

Trabalho de Conclusão de Curso – Artigo Científico, apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Prof. Esp. Alyne Leite de Oliveira

JUAZEIRO DO NORTE-CE
2024

SANIELLY AUREA DE SOUZA MARTINS

DEEPFAKE E A VIOLAÇÃO AO DIREITO DA PERSONALIDADE: análise da percepção de pessoas na cidade de Juazeiro do Norte-CE

.

Data da Apresentação 01/07/2024

BANCA EXAMINADORA

Orientador: Prof. Esp. Alyne Leite de Oliveira

Membro: Prof. Esp. Francisco Gledison de Lima Araújo/UNILEÃO

Membro: Prof. Esp. Antonio Raniel Silva Lima/UNILEÃO

JUAZEIRO DO NORTE-CE
2024

DEEPFAKE E A VIOLAÇÃO AO DIREITO DA PERSONALIDADE: análise da percepção de pessoas na cidade de Juazeiro do Norte-CE

Sanielly Aurea de Souza Martins[1]
Alyne Leite de Oliveira[2]

RESUMO

As *Deepfakes* possuem a capacidade de forjar vídeos, principalmente, criando situações fictícias onde determinados indivíduos têm sua face substituída através de uma sobreposição do sistema da "IA" sem que haja o consentimento para tal utilização. Com a grande exposição no mundo digital, as pessoas têm acesso a esse tipo de conteúdo de maneira fácil e rápida, e por esse motivo, torna-se perigosa a disseminação de vídeos e áudios falsos, bem como sua veiculação, criados, muitas vezes, intencionalmente, para prejudicar determinada pessoa. Considerando esses aspectos, o presente estudo visa analisar a percepção de pessoas da cidade de Juazeiro do Norte-CE acerca das *deepfakes* e suas consequências jurídicas e sociais. Como objetivos específicos delineou-se: compreender o fenômeno das *deepfakes*; identificar quais direitos são violados a partir de sua utilização e criação, assim como os impactos sociais e jurídicos gerados. Por meio de um levantamento teórico e aplicação de uma pesquisa do tipo *survey* aplicada por meio de redes sociais a pessoas da região metropolitana do Cariri-CE, foi possível dimensionar a relevância deste. Percebe-se, com a realização deste, que o público investigado não apenas utiliza-se de tecnologia como de ferramentas de inteligência artificial, como conhecem e compreendem o fenômeno *deepfake*, porém se percebe que a compreensão acerca dos riscos, regulamentação e pena ainda deixam a desejar, o que deixa brechas para utilizações indevidas.

Palavras Chave: *Deepfake*. Inteligência Artificial. Direitos da Personalidade.

ABSTRACT

Deepfakes have the ability to forge videos, mainly by creating fictitious situations where certain individuals have their face replaced through an overlay of the "AI" system without consent for such use. With the great exposure in the digital world, people have access to this type of content easily and quickly, and for this reason, the dissemination of fake videos and audios, as well as their dissemination, often created by intentionally to harm a specific person. Considering these aspects, the present study aims to analyze the perception of people in the city of Juazeiro do Norte-CE regarding deepfakes and their legal and social consequences. The specific objectives were outlined: understanding the phenomenon of deepfakes; identify which rights are violated through its use and creation, as well as the social and legal impacts generated. Through a theoretical survey and the application of a survey-type research applied through social networks to people in the metropolitan region of Cariri-CE, it was possible to assess its relevance. It is clear, with the completion of this, whatthe investigated public not only usesof technology asof artificial intelligence tools, as they know and understand the deepfake phenomenon, but it is clear that the understanding of the risks, regulations and penalties still leaves something to be desired, which leaves room for misuse.

Keywords:*Deepfake*. Artificial intelligence. Personality Rights.

[1] Graduanda do Centro Universitário Doutor Leão Sampaio/Unileão_
[2] Professora Orientadora do Centro Universitário Doutor Leão Sampaio/Unileão, mestranda em Direito da Empresa e dos Negócios/Unisinos_alyneoliveira@leaosamapio.edu.br

1 INTRODUÇÃO

Devido ao avanço da tecnologia e sua multifuncionalidade, se tornou possível a prática de crimes cibernéticos, popularmente conhecidos como crimes de internet, caracterizando-se pela atividade delituosa, cujo alvo é um dispositivo eletrônico (computador, celular, tablet, dentre outros), que esteja ligado à rede.

Assim, considera-se um cibercrime, por exemplo, a fraude, o furto e o estelionato, desde que praticados mediante a internet (ALGAR, 2022). Porém, além desses crimes virtuais, utilizados por meio de um dispositivo eletrônico, surgiu o chamado *deepfake*, caracterizando-se por sua criação e manipulação de imagens – fotos, vídeos e/ou sons - áudios. Trata-se de uma forma avançada de adulteração de mídia digital e vem ganhando destaque nos últimos anos, haja vista que, desde suas aplicações iniciais, essa tecnologia revolucionária tem gerado diversos debates (TECMUNDO, 2023).

Por conseguinte, o estudo sobre *deepfake*s é um campo que há muito a ser explorado, posto que à medida que o processo de criação se torna mais sofisticado, a capacidade de identificá-los se torna cada vez mais complexa. Nesse cenário, de acordo com um estudo da *University College London* (UCL), em torno de 73% das vezes foi possível ser identificado uma *deepfake* por um ser humano, de modo que as abordagens para sua detecção incluem a análise de artefatos de processamento de imagem, a verificação da autenticidade dos metadados e o uso de redes neurais para identificar padrões de manipulação. Neste sentido, como conclusão, os pesquisadores entenderam que treinar seres humanos para detecção de *deepfakes* não é eficiente, não obstante os *softwares* tenham errado em 25,3% das ocasiões (O GLOBO, 2023).

O cenário apresentado, com a criação de conteúdos áudio e visual, foco do *deepfake*, o direito a imagem se mostra violado de maneira excessiva, bem como o direito à honra e à privacidade, uma vez que há tamanho constrangimento para a vítima e sua utilização de maneira maliciosa causa danos em potencial para os envolvidos (OLHAR, 2023).

O que se percebe, no entanto, é que há ainda um conhecimento limitado da população acerca deste fenômeno, dado o intenso uso de redes sociais, que muitas vezes se confunde com algo rotineiro e até sem sua devida relevância.

Observe-se que é assegurado constitucionalmente direto à imagem, honra, personalidade, privacidade, dentre outras e, em contraposição a esses direitos há a incidência da *deepfake*, objeto do presente estudo, que, violam direitos inerentes à pessoa natural, direitos

esses que são considerados fundamentais.

Nesse diapasão, questiona-se qual o nível de conhecimento da população do Juazeiro do Norte sobre o *deepfake*?

Portanto, tem-se como objetivo geral analisar a percepção de pessoas da Região Metropolitana do Cariri-CE acerca das *deepfakes.* e suas consequências jurídicas e sociais, apresentando-se como específicos: a) compreender o fenômeno das *deepfake*s; b) Identificar quais direitos são violados a partir de sua utilização e criação, assim como os impactos jurídicos e sociais gerados.

Outrossim, o estudo mostra-se relevante haja vista que, segundo a Agência Pública, baseando-se em dados fornecidos pela *Impressions App* (aplicativo) o Brasil é o 2° maior público na utilização da plataforma – Synthesized (aplicativo) possuindo um total de 20% de usuários. De acordo com um estudo com a Sensitivity, uma empresa americana, 95% das *deepfakes* do ano de 2019, eram de vídeos falsos de atos sexuais não consensuais (PUBLICA, 2020). Ademais, cerca de 65% dos brasileiros não sabem o que é "*deepfake*", conforme a *perallis security,* empresa de cibersegurança, não obstante sejam alarmantes os dados de sua crescente veiculação. Portanto, a ampliação de estudos e discussões sobre o tema mostram-se prementes, a fim de retardar ou minimizar os impactos frente à sociedade e, em especial, as vítimas e envolvidos.

Por fim, trata-se de uma pesquisa de natureza básica, exploratória, descritiva, quantitativa, tendo como método o *survey,* por meio da aplicação de pesquisa de opinião virtual dentre a população da cidade de Juazeiro do Norte/CE.

2 REFERENCIAL TEÓRICO

Para que sejam abordados a composição que o presente estudo se propõe, se faz necessário, inicialmente, entender as noções históricas básicas acerca da inteligência artificial e seus avanços na sociedade, bem como, sua violação aos direitos da personalidade.

2.1 AVANÇOS TECNOLÓGICOS

A origem tecnológica se deu na pré-história, quando ancestrais começaram a ampliar técnicas, bem como, ferramentas para se desenvolverem. Durante o período da Idade Média, muitos avanços ocorreram, como áreas da arquitetura, agricultura e engenharia, além do desenvolvimento de novas técnicas para produção de metais. A revolução cientifica, entre

meados 1820 e 1840, provocou grande saltos nas áreas da física, astronomia, medicina, saúde e economia (ORIGEM, 2023).

No século XX, houve avanços tecnológicos significativos em diversas áreas, em especial na televisão, computadores, telefones e internet, que ocorreu com a chegada da Revolução da Informação e as Telecomunicações ou Era da Informação, que ocorreu entre 1985 a 2000 (STOODI, 2020). Enquanto no século XXI tem sido caracterizado pelo avanço da tecnologia da informação e comunicação, com o advento da internet, das redes sociais e da inteligência artificial.

Para Cardoso (1996), a revolução do século XX foi a fusão da ciência, tecnologia com a liberdade; e da universidade sendo possível grandes revoluções tecnológicas que vão desde a criação da energia nuclear até a biotecnologia, computadores, microeletrônica e robótica.

A partir de 2000, o desenvolvimento global tornou-se mais evidente, devido o crescimento tecnológico. Onde, além da participação dos Estados Unidos e Europa, a China começou a se destacar. Segundo Friedman (2007), embora a China possuía a maior economia do século XVIII, foram os países e empresas ocidentais que fizeram a maior parte da formação e globalização do sistema, entretanto, será cada vez mais incomum no futuro. À medida que a globalização 3.0, para o autor Pankaj Ghemawat, achata e encolhe o mundo, será cada vez mais impulsionada por um grupo mais diversificado de indivíduos e não apenas por alguns, sendo eles cada vez mais empoderados. A globalização 3.0 permite que mais pessoas se conectem e joguem, sendo possível analisar todas as cores do arco-íris humano participando.

Cabe-se destacar que a Nova Globalização é um novo processo pelo qual os países estão passando, relacionado à revolução tecnológica que intensifica cada vez mais o relacionamento entre os países, cujo os cidadãos estão altamente conectados globalmente, com clientes e fornecedores globalmente conectados (BDM, 2019).

Nos tempos atuais, a tecnologia permanece em constante transformação. A tecnologia da informação é uma das mais importantes atualmente, além de abrangente, pois engloba o uso de computador, *smatphones* e *softwares*, possuindo grande relevância na comunicação célere com outras pessoas (CNN, 2023).

Para Kai-Fu Lee, no seu livro “Inteligência Artificial”, o avanço tecnológico refere-se ao progresso contínuo ao longo da história e às inovações que ocorrem em diversas áreas da ciência e da engenharia, resultando em melhorias significativas em produtos, processos e serviços. A inteligência artificial é um dos campos que tem impulsionado fortemente o avanço tecnológico nas últimas décadas, permitindo o desenvolvimento de sistemas e aplicações cada vez mais sofisticados e capazes de realizar tarefas complexas e multiformes, impactando

profundamente diversos setores da sociedade, impulsionando a inovação, a eficiência e a qualidade de vida.

2.2 INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial (IA) é um campo da ciência da computação que se concentra no desenvolvimento de sistemas e máquinas capazes de realizar tarefas analíticas e manuais que, normalmente, exigiriam inteligência humana, como reconhecimento de padrões, aprendizado, visão computacional e muito mais, conforme pré-configuração previamente estabelecida pelo desenvolvedor do sistema. A “IA” busca replicar processos cognitivos humanos, como aprendizado, raciocínio e resolução de problemas, utilizando algoritmos e modelos matemáticos complexos, ou seja, simulando a inteligência humana, aproximando-se ao máximo da realidade (LEE, 2019).

De acordo com Fabiano Hartmann Peixoto e Roberta Zumblick Martins da Silva (2019, p. 20), a inteligência artificial baseia-se em: “[...] solucionar dado problema, resolvendo-o, raciocinando e aprendendo com as situações”.

O termo “Inteligência Artificial” surgiu em meados de 1955, por John MacCarthy, e segundo ele, caracteriza-se como "É a ciência e engenharia da criação de máquinas inteligentes, especialmente programas de computação inteligentes. Está relacionado à tarefa semelhante de usar computadores para entender a inteligência humana, mas a IA não precisa se limitar a métodos de observação biológica" (STUDIO, 2016).

Considera-se a mudança tecnológica mais desenvolvida da área da ciência da computação, através dele, é possível conectar numerosos ambientes da vida como casa, trabalho e lazer em uma única experiência. A IA irá auxiliar para prever necessidades do cotidiano, lembrar de determinadas tarefas, ensinar como realizar determinadas atividades, bem como sua automação, dentre outros (BLIP, 2023).

Para Fabio G. Cozman e Hugo Neri (2021, p. 21) tal tecnologia pode ter um caráter mais específico: “[...] sistema que pensam como humanos; que agem como humanos; que pensam racionalmente, que agem racionalmente (implícito aqui o ponto que humanos nem sempre pensam/agem racionalmente[...]”.

A IA encontra-se em desenvolvimento tangencial, se assemelhando com atividades e características essencialmente humanas, dividindo-se primordialmente em 4 tipos. O primeiro, é conhecido como *Machine Learning*, onde se concentra no desenvolvimento de algoritmos que permitem aos computadores aprender com dados e experiências passadas, ou seja, baseado no

que foi acessado anteriormente (LATINO, 2022).

A próxima, é a *Deep Learning***,** essa abordagem possibilita o reconhecimento de padrões e o processamento de informações de maneira mais efetiva, ao extrair referências de determinados conjuntos de dados, que podem ser treinados para reconhecer padrões complexos nos dados (LATINO, 2022).

Já o Processamento de Linguagem Natural (PLN)**,** desenvolve algoritmos e técnicas que capacitam os computadores a ler, compreender e interpretar, conforme a capacidade humana. Por último, a Visão Computacional**,** é como instruir um equipamento computadorizado a enxergar o mundo como um ser humano visualiza, sendo aplicado a diversos cenários do cotidiano, seja em áreas da saúde, educação, lazer, empreendedorismo, e muito mais (LATINO, 2022).

A inteligência artificial (IA) é considerada “a quarta revolução industrial” se fazendo cada vez mais presente na vida em sociedade, retrata a tamanha modernidade nos tempos atuais, e com isso, realidades nunca antes vivenciadas, podendo ser encontrada em diversas áreas, tais como ferramentas, equipamentos, sejam celulares, *chatbots*, internet banking, jogos eletrônicos e dentro outros, impactando significativamente na forma que as pessoas vivem, uma vez que seu uso visa automatizar tarefas repetitivas e rotineiras, aumentando a eficiência e a produtividade. Empresas estão utilizando algoritmos para personalizar serviços e produtos de acordo com as preferências e necessidades individuais dos consumidores, sendo aplicada também na área da saúde para auxiliar no diagnóstico de doenças, identificação de padrões em exames médicos e desenvolvimento de tratamentos mais assertivo. Na educação está sendo empregada na personalização do ensino, adaptando o conteúdo educacional às demandas particulares dos alunos. (LEE, 2019).

Essa evolução apresenta mudanças abruptas à sociedade em termos de desenvolvimento e avanços, materiais, tecnológicos e científicos, porém, pode significar novos desafios no tocante ao que dela advém, como as *deepfake*s.

2.3 *DEEPFAKE*

Deepfake é uma técnica de inteligência artificial que combina, sobrepõe ou funde imagens e vídeos existentes com outras imagens ou vídeos, para criar conteúdo multimídia falso e aparentemente legítimo. É realizado através de algoritmos de aprendizado para analisar e sintetizar padrões complexos em dados visuais. Permitindo criar ou recriar situações irreais, com a utilização de imagens, vídeos e áudios. O termo "*deepfake*" é uma junção de "deep

learning" (aprendizado profundo) e "fake" (falso) (CNN, 2022).

Segundo Stuart Russell (2021), no livro “Inteligência artificial a nosso favor: como manter o controle sobre a tecnologia”, o *deepfake* é caracterizado pela criação de vídeo e áudio, através da Inteligência Artificial, para que determinada pessoa faça ou diga qualquer coisa, onde, no campo real não aconteceu de fato. Russel alerta sobre a produção desse tipo de ferramenta quanto a sua aplicação para veiculação de notícias falsas, bem como, identidades falsas.

No livro em questão, Russell (2021) aponta que a combinação de IA, gráficos de computadores e síntese de fala tem permitido a criação de *deepfake*s, que são conteúdos de vídeo e áudio realista de praticamente qualquer pessoa dizendo ou fazendo determinada coisa. A tecnologia permite que pessoas em todo mundo usem o evento, que só precisa ser descrito verbalmente. Imagens capturadas por telefone do senador X aceitando suborno do traficante de cocaína Y no lugar do suspeito Z? Não há problemas! Além disso, esse tipo de conteúdo tem o potencial de criar crenças persistentes em coisas que nunca aconteceram. Além disso, sistemas de IA tem a capacidade de criar milhões de identidades falsas, conhecidas como “*armies* robóticas”, que tem a capacidade de criar bilhões de comentários, tuítes e sugestões em um ritmo acelerado. (RUSSEL, 2021).

São produtos de programas que se utilizam da capacidade de “aprender” conteúdo de mídia digital, seja com imagens, vídeos, áudios para simular a realidade utilizando mecanismos artificiais para replicar características humanas, como voz, expressões faciais e movimentos corporais. Ou seja, é possível adulterar o rosto de uma pessoa em fotos ou vídeos por meio da inteligência artificial (CORREIO, 2022).

A *deepfake* possui uma vasta gama de aplicações. Desde utilização na indústria cinematográfica para auxiliar nas produções, melhorando a qualidade de vídeo, criação de efeitos visuais e dublagens de filmes estrangeiros, com a finalidade de entretenimento. Entretanto, tal tecnologia traz preocupações devido à natureza enganosa utilizada, muitas das vezes (CNN, 2022).

Encontra-se disseminada principalmente em sites pornográficos, onde são criadas situações que nunca foram vivenciadas por aquela pessoa, muito menos sem que haja sua autorização. O impacto que esse tipo de conduta traz na vida de uma pessoa, é imensurável. Ou seja, se resume em uma tecnologia baseada em uma IA, onde é realizado a sobreposição de um rosto, ao corpo de outra pessoa, para que o vídeo retrate uma falsa realidade, podendo não só abordar alteração de imagens visuais, mas também da voz do indivíduo. Observando esse cenário, a regulamentação legal se torna fundamental, pois é imprescindível que o ordenamento

jurídico brasileiro seja eficiente na tratativa do tema (KASPERSKY, 2019).

Os danos causados pelos *deepfakes* são diversos e podem afetar diferentes aspectos da sociedade. Podem ser usados para criar e disseminar informações falsas, manipulando a opinião dos usuários, levando à perda da confiabilidade de mídias digitais, tornando mais difícil identificar entre o que é real e o que é falso. Caso sua criação possua o objetivo de difamar ou caluniar alguém, isso pode causar danos irreparáveis e incalculáveis à reputação da pessoa afetada (LBCA, 2024).

De tal modo, embora haja diversos benefícios e facilidades ao cotidiano, faz-se necessário assegurar direitos e deveres para os cidadãos, evitando que não haja quaisquer violações.

2.4 CRIMES CIBERNÉTICOS

Os crimes cibernéticos ou ciber crimes (em inglês, *cybercrimes*), são toda e qualquer atividade ilícita praticada na internet, por meio de dispositivos eletrônicos como smartphones e computadores. O primeiro registro da nomenclatura cibercrime ocorreu no final da década de 1990, durante um encontro de líderes do G-8, o grupo dos oito países mais ricos e influentes do mundo, quais sejam, Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia (FIA, 2021).

Os *cybercrimes* tem como objetivo corromper, através de um malware, os dispositivos ou impedi-los de funcionar. Existe a possibilidade, também, de excluir ou roubar dados pessoais através desse mecanismo. Ademais, podem impedir os usuários de usar um site ou rede ou impedir que uma empresa forneça um serviço de software a seus clientes.

Segundo Marco Aurélio Rodrigues da Costa (1995), os crimes virtuais se dividem em puros, mistos e comuns. O crime informático puro é aquele que se encontra relacionado a um sistema de computação, onde o objetivo principal é corromper os dados, utilizando por exemplo, um *software* ou *hardware*. O crime informático misto, ocorre da violação do bem jurídico, ou seja, a partir da consumação do delito, como por exemplo, furto eletrônico. O crime informático comum é aquele que está tipificado no ordenamento jurídico, podendo ou não ocorrer por intermédio de um dispositivo eletrônico, como por exemplo, pedofilia, racismo e *cyberbullying* (CAMPO, 2019).

Os crimes cibernéticos estão aumentando ano após ano. De acordo com o relatório Estado da resiliência da segurança cibernética de 2021 da Accenture, os ataques de segurança tiveram um aumento de 31% de 2020 a 2021 (KOBOLDT, 2023).

Diante dos crimes acima definidos, no ano de 2012 uma nova lei ganhou notoriedade, recebendo o nome de Lei Carolina Dieckmann, lei federal de n° 12.737/2012. Surgindo, portanto, através do computador da referida atriz, sendo divulgado arquivos pessoais, dentre eles, fotos íntimas, se tornando público. A partir a referida lei, o Código Penal sofreu alteração, acrescendo, os artigos 154-A e 154-B, e sendo também alterados os artigos 266 e 298.

O artigo 154-A tipifica o crime de invasão de dispositivo informático, conectado ou não à rede de computadores, violando a sua segurança, com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização do titular.

A fraude online é considerada um crime cibernético, pois pode incluir esquemas de *phishing*, utilizada por criminosos que tentam obter de forma ilegal informações pessoais e financeiras, e fraudes de comércio eletrônico, onde bens ou serviços são oferecidos, mas nunca entregues (DESKTOP, 2024).

Como também, o roubo de identidade, ao obter de forma ilícita e não consensual informações pessoais, como números de segurança social, datas de nascimento e números de cartão de crédito, para cometer fraudes financeiras ou outros crimes (DESKTOP, 2024).

São crimes, por conseguinte, os Ataques de Malware e Ataques de Negação de Serviço (DDoS). Onde o primeiro consiste na distribuição de *software* malicioso, como vírus, *worms*, *ransomware* e cavalo de troia, geralmente ocorre através de um link ou um anexo de email, que podem danificar sistemas de computador ou dispositivo, além de qualquer aparelho que venha a se conectar a ele, com a finalidade de roubar informações ou extorquir dinheiro. Já o segundo, um tipo de ataque é uma tentativa maliciosa que sobrecarrega um servidor, serviço ou rede com um grande volume de tráfego, tornando-o inacessível para os usuários (FIA, 2021).

Já a ciberespionagem, envolve o roubo de informações confidenciais de indivíduos, empresas e/ou governos, por meio de ataques direcionados ou infiltrando-se em redes de computadores, com o objetivo de divulgar e alterar dados (JUSBRASIL, 2024).

No mundo virtual, consegue-se identificar *cyberbullying* e Assédio Online, utilizando da tecnologia através de programas, sites, celular, por exemplo, para assediar, intimidar, insultar ou difamar outras pessoas, violando diretamente a intimidade do usuário (FIA, 2021).

Além de tal, o alto fluxo de Pornografia Infantil Online, consistindo na produção, distribuição, armazenamento ou consumo de imagens e vídeos pornográficas de crianças e adolescentes, geralmente compartilhadas através da internet (TJDFT, 2017).

Ao realizar uma breve exposição de alguns crimes cibernéticos, não se pode deixar de mencionar a invasão de privacidade da vítima, onde a mesma sofre interceptação não autorizada

de comunicações eletrônicas, a invasão de contas online ou a espionagem de dispositivos eletrônicos.

No livro "AI Superpowers" de Kai-Fu Lee (2018), a ética e a regulamentação da inteligência artificial, levando em consideração princípios éticos, morais e legais, considera-se a necessidade de estabelecer políticas, leis e diretrizes que orientem o desenvolvimento e o uso da inteligência artificial, protegendo os direitos individuais e promovendo a segurança e a confiança na tecnologia. Esses temas refletem a complexidade e a importância de considerar aspectos éticos e regulatórios, visando garantir que essa tecnologia seja desenvolvida e aplicada de maneira ética, responsável e benéfica para a sociedade como um todo, bem como a garantia do direito de personalidade.

2.4 DIREITOS DA PERSONALIDADE

Os direitos da personalidade são fundamentais à pessoa humana, para que assim possa determinar o tratamento justo e igualitário na sociedade com as demais pessoas. Os direitos intrínsecos aos indivíduos, compreendem seu corpo, sua imagem, seu nome, e todos os aspectos que caracterizam sua identidade.

Para se entender melhor a respeito de suas violações, precisa-se primeiro, conceituar quais são os direitos da personalidade.

Conforme frisa o art 5°, inc. X da CF/1988, são invioláveis a intimidade, vida privada, honra e imagem, sendo resguardado o direito a indenização pelo dano moral ou material decorrente de sua violação.

As violações do direito da personalidade através da *deepfakes* podem incluir, a Difamação e Calúnia, se o objetivo for para criar vídeos ou imagens falsas que difamam ou caluniam uma pessoa, isso pode constituir uma violação do direito à reputação. Além da Violação da Privacidade, caso as imagens ou vídeos íntimos são manipulados para criar *deepfakes* sem consentimento, isso pode ser considerado uma violação da privacidade da pessoa envolvida.

O Uso Indevido de Imagem também é uma violação, tendo em vista a utilização da imagem de uma pessoa sem sua autorização pode violar seu direito de controle sobre sua própria imagem. Bem como, o Dano à Honra e à Dignidade, ao criar uma falsa realidade para ridicularizar ou humilhar uma pessoa, isso pode infringir seu direito à dignidade. Além do Assédio e Intimidação: *Deepfake*s podem ser usados para assediar ou intimidar uma pessoa,

causando danos emocionais e psicológicos

A dignidade humana não consiste em uma conceituação padronizada, sua percepção quanto a essencialidade ao ser humano se modifica conforme a cultura e a história de cada sociedade, bem como suas concepções particulares de vida de cada indivíduo. Sua consagração no cenário internacional e sua inserção à Constituição brasileira de 1988 culminando além do direito civil, o direito privado. O Código Civil dedicou-se aos direitos da personalidade, em onze artigos (arts. 11a 21), buscando regulamentar o direito ao próprio corpo, ao nome, à honra, à imagem e à privacidade (SCHREIBER, 2013).

O tratamento jurídico quanto ao corpo humano sofreu influência da religião. O século XX levantou a necessidade de estabelecer garantias legais contra intervenções, sofridas por meio da tortura e experimentação científica. Sendo possível, por meio de normas jurídicas nacionais e internacionais assegurar proteção à integridade física e psíquica do ser humano. A Constituição brasileira de 1988, reconhece o direito à integridade psicofísica, já o Código Civil de 2002 limitou-se, a contemplar o direito à integridade psicofísica quanto aos atos de disposição do corpo humano, em outras palavras, a relação entre a proteção ao corpo e a vontade do seu titular (SCHREIBER, 2013).

A violação do direito à honra compreende-se a reputação da pessoa em seu meio social, muitas vezes, vem acompanhada do uso não autorizado da imagem, podendo ser vista sem o suo da imagem ou do nome, como na hipótese se lhe ser destinado um xingamento vexatório em um ambiente público, ofendendo à honra e à respeitabilidade (SCHREIBER, 2013).

O direito à imagem independe, portanto, do direito à honra. Esse, por sua vez detém representação audiovisual da sua individualidade, podendo ser constituída por instrumentos técnicos de captação, registros computadorizados, bem como pela ação artística da criatividade, como por exemplo, filmes e telas de pintura. O uso não consentido da representação da pessoa, por si só, atribui violação ao direito de imagem, cuja regulamentação encontra-se devidamente reconhecida na Constituição Federal, ressaltando a inviolabilidade a intimidada, vida privada, honra e imagem. No cenário atual, vislumbramos uma sociedade efêmera por alta exposição pública e pela transmissão de informações em tempo real, apresentando dificuldades marcantes quanto a tutela da imagem do indivíduo frente a coletividade (SCHREIBER, 2013).

Em uma sociedade caracterizada pelo constante intercâmbio de dados, o direito à privacidade deve se propor além da proteção à vida íntima, cuja finalidade inicial era presumida. Necessitando abranger também o direito de manter o controle sobre os seus dados pessoais, a intervenção na intimidade doméstica, suas características físicas, código genético, estado de saúde, crença religiosa, o fornecimento de dados fornecidos ou coletados de forma

aparentemente sutil e inofensiva, ou qualquer outra informação pertinente à pessoa. O uso inadequado desses dados pessoais pode gerar diversos prejuízos ao seu titular. É nesse sentido que se emprega normalmente a expressão invasão de privacidade, ultrapassando a esfera de intimidade, hoje, sendo assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação. Entretanto, o desafio atual da privacidade não está na sua afirmação, mas na sua efetividade (SCHREIBER, 2013).

A concepção rígida do nome, como sinal distintivo imodificável, foi implementada pela legislação brasileira. Permite-se, hoje, a retificação da grafia do nome decorrente do erro no registro, a tradução do nome estrangeiro nos casos de naturalização, a alteração do prenome suscetível de expor o seu titular ao ridículo, a adaptação do prenome com a inclusão de apelido público notório, a alteração do nome devido a adoção, e assim por diante. O que a legislação consagra expressamente não é um direito, mas um dever ao nome. A Lei de Registros Públicos determina a indicação de um nome para toda pessoa desde o seu nascimento, uma vez somos confrontados a todo instante com uma exigência de identificação pelo nome em praticamente, todos atos solenes da vida civil. Não sendo lícito que qualquer pessoa deixe ter um nome, parece bastante evidente que o nome é antes um dever que um direito. A doutrina italiana desenvolveu, a partir da década de 1970, o direito à identidade pessoal, que abarca a proteção ao nome, em outras palavras, um direito de 'ser si mesmo' *(diritto ad essere se stesso*), entendido como o respeito à imagem da pessoa meio a vida em sociedade, experiência pessoais, a aquisição de ideias, convicções morais, sociais e religiosas, morais e sociais que diferenciam a pessoa e ao mesmo tempo a qualificam. Sua identidade pessoal não deve apenas ser vista como demandas indenizatórias, mas também como diretriz de iniciativas sociais, alcançados pela realização da dignidade humana (SCHREIBER, 2013).

No Código Civil brasileiro de 2002, nos arts. 11 ao 21, compreendem-se os direitos ao corpo, nome, imagem e a vida privada. Com a grande veiculação nas redes sociais, vive-se em um cenário de incertezas, com a constante ameaça da violação dos direitos da personalidade de outrem, com a criação e divulgação da imagem, vídeos e da fala de indivíduos de forma deformada e inverídica.

A jurista Chiara Spadaccini de Teffé (2016), aponta alguns possíveis desdobramentos do uso de tais tecnologias e a modernidade ligadas, com a evolução da tecnologia, surgem novas ferramentas que podem causar danos a outras pessoas, como a divulgação não autorizada de imagens íntimas em aplicativos, bem como sites de compartilhamento de conteúdo, além da criação de perfis falsos em redes sociais; organização de conteúdo inadequado pelos provedores de pesquisa; criação de páginas com mensagens ofensivas sobre alguém; exposição abusiva da

imagem em notícias ou programas de humor. Além disso, práticas como o *cyberbullying* e a pornografia de vingança estão relacionadas ao uso indevido de imagens na internet.

Para Teffé (2017), ao passo que a tecnologia avança e se desenvolve, se torna mais propício o surgimento de novas ferramentas capazes de causar dano a determinado indivíduo, violando o seu direito a personalidade, devidamente protegido por lei. A veiculação de imagens íntimas, cenas de nudez em sites pornográficos e aplicativos, tem se tornado cada vez mais comum e corriqueiro.

Os direitos da personalidade estão tipificados no Capítulo II do Código Civil Brasileiro (Lei n° 10.406/2002), compreendidos nos arts 11 ao 21 abarcando os direitos ao corpo – quando importar diminuição permanente da integridade física – nome, imagem – se lhe atingirem a honra, boa fama ou a respeitabilidade, e a vida privada.

Além da complexidade quanto ao uso e a veiculação das *deepfakes*, o seu alcance torna o cenário mais delicado, onde, evidencia-se a carência de regulamentação sobre o tema em questão, uma vez que o potencial danos tem se tornado cada vez mais elevado.

Para Anderson Shireiber (2014), o uso indevido de imagem, invasão à privacidade, furto de dados pessoais, são exemplos de perigos que cercam a condição humana, onde tais perigos, na prática jurídica ensejam a uma vasta gama de conflitos.

A legislação atual brasileira não criminaliza o "*Deepfake*", entretanto, os intérpretes vêm buscando amparo buscando como base os tipos penais presentes nas leis Lei Federal n.º 12.737/2012 popularmente conhecida como Lei Carolina Dickmann, Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, crimes contra a honra (artigos 138/145 do Código Penal) e dignidade sexual (artigos 213/235 'c' do Código Penal).

Em muitos países, existem leis e regulamentações que abordam essas questões, mas a natureza emergente e altamente técnica dos *deepfakes* pode apresentar desafios para a aplicação eficaz dessas leis. Portanto, é importante que os sistemas legais se adaptem para lidar adequadamente com esse tipo de violação do direito da personalidade.

Em meio aos avanços tecnológicos e aos desafios da privacidade, a proteção dos dados pessoais tornou-se uma questão essencial. É importante que governos, empresas e indivíduos reconheçam a importância de garantir a confidencialidade, integridade e disponibilidade dos dados pessoais. Por essa razão, se fez necessário criar uma lei, visando a proteção e segurança dos usuários. A Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018), tem como finalidade principal a proteção os direitos fundamentais, da liberdade, privacidade e personalidade. Visa, também, a segurança jurídica para garantir a proteção aos dados pessoais de todo cidadão. (JURID, 2023)

A LGPD estabelece regras e princípios para a administração de dados pessoais, com o objetivo de proteger a privacidade e a liberdade dos cidadãos. Estabelece que as empresas necessitam obter consentimento explícito dos indivíduos para coletar, utilizar e armazenar seus dados, devendo garantir que tais informações sejam armazenadas de forma segura. O não cumprimento das disposições da LGPD pode resultar em penalidades, como multas e sanções. (MPF, 2020)

3 MÉTODO

A presente pesquisa possui natureza básica exploratória, dispondo quanto aos objetivos de maneira descritiva, detendo à abordagem do problema de forma quantitativa, conforme as fontes bibliográficas, abrangendo o procedimento *survey*, na região do Cariri cearense.

Pode-se afirmar que a pesquisa é fundamental, já que busca satisfazer a necessidade de adquirir conhecimento, dispensando a obrigação de ter uma aplicação prática específica, mas abrangendo verdades e interesses globais. Logo, Andrade (2010, p. 110) aduz que "o objetivo da pesquisa é alcançar o saber, para a satisfação do desejo de adquirir conhecimentos", uma vez que essa compreensão permitirá ampliar as possibilidades de resolver os fenômenos em estudo, assim como é proposto no atual projeto de pesquisa.

No que diz respeito aos objetivos, se está diante de uma investigação exploratória e descritiva, a qual, como ensina Gil (2018), visa elucidar o problema, permitindo maior compreensão da realidade enfrentada pela sociedade. Além disso, essa deve ser a etapa inicial planejada na pesquisa.

Neste sentido, nota-se a correlação entre o tipo de pesquisa e o objetivo estabelecido, já que o propósito deste estudo é se aproximar ao máximo do tema, buscando compreender amplamente o fenômeno da adoção tardia por meio da visão popular.

Quanto ao método empregado, trata-se de um *survey*, que, segundo Fowler (2011), tem como propósito fornecer descrições estatísticas das pessoas por meio de questionamentos, geralmente aplicados em uma amostra. É importante ressaltar ainda que os pesquisadores de *survey* querem obter o máximo de compreensão com o mínimo de variáveis possíveis; portanto, eles podem criar vários modelos explicativos e então escolher o que melhor funciona para seus objetivos.

A escala Likert de cinco pontos de concordância e frequência foi utilizada para levantamento dos dados por meio de um formulário estruturado com perguntas fechadas. "As escalas Likert são ótimas para se aprofundar em um tópico específico para descobrir (em mais

detalhes) o que as pessoas pensam sobre ele" (FRANÇA, 2021).

Quadro 1: Escalas utilizadas na coleta de dados

Valor equivalente	Concordância	Frequência
1	Discordo Totalmente	Nunca
2	Discordo	Raramente
3	Não estou decidido	Ocasionalmente
4	Concordo	Frequentemente
5	Concordo Totalmente	Muito Frequente

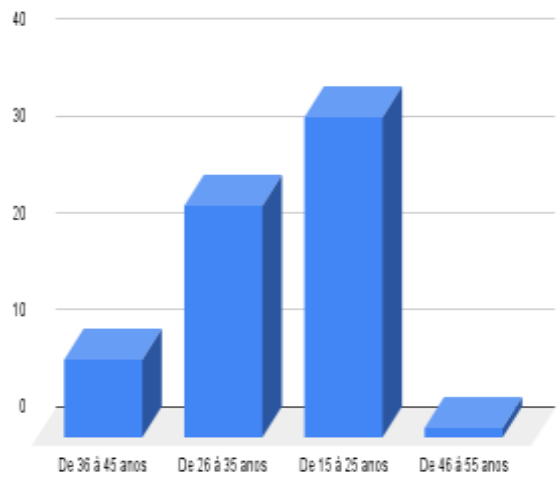
Fonte: Adaptado de França (2021).

O levantamento foi feito durante o mês de junho de 2024, por meio de plataformas virtuais, onde 66 (sessenta e seis) pessoas responderam ao questionário, cuja criação se deu por meio o *Google Forms*, sendo divulgado via *WhatsApp*

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

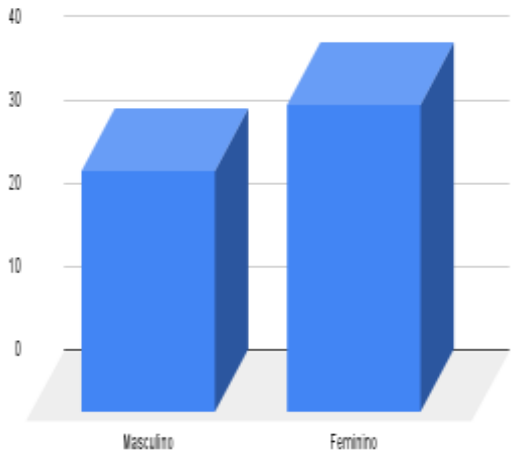
Considerando-se o objetivo proposto por este estudo, os dados levantados demonstram uma limitação em relação à quantidade de pessoas abrangida no período de coleta, porém estes serviram como parâmetro para observação da percepção das pessoas que estão imersas em um contexto tecnológico e os riscos aos quais estão expostos.

Gráfico 1: Idade



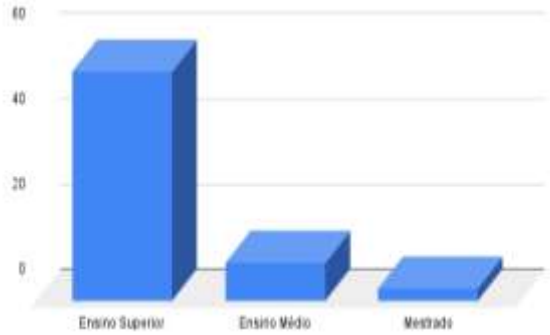
Fonte: Dados da Pesquisa (2024).

Gráfico 2: Gênero



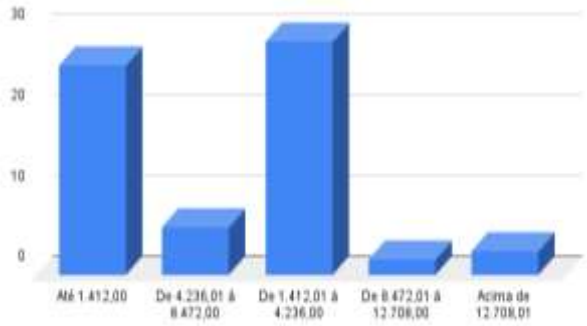
Fonte: Dados da Pesquisa (2024).

Gráfico 3: Formação



Fonte: Dados da Pesquisa (2024).

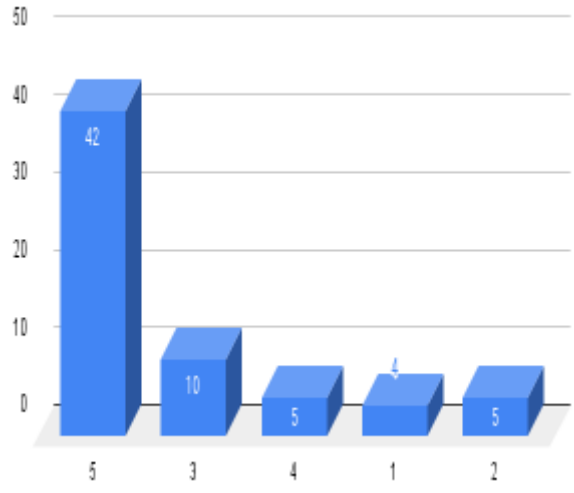
Gráfico 4: Renda



Fonte: Dados da Pesquisa (2024).

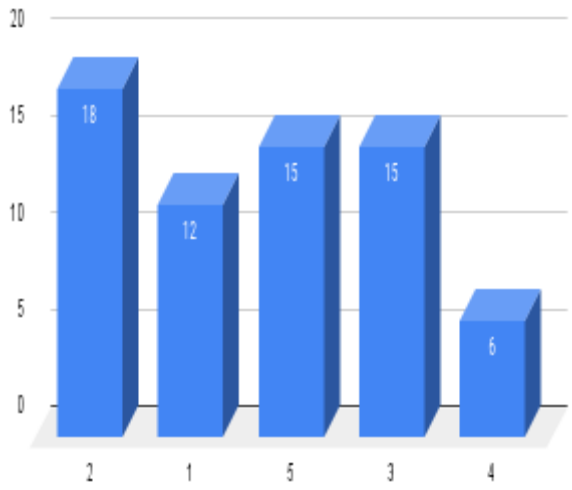
Dentre os participantes do estudo há uma predominância do sexo feminino (56,1%), com idade entre 15 e 21 anos (50%) e 26 à 35 anos (36,4%). O público se destaca por estar no ensino superior (81,8%). A renda varia entre um público cuja renda é até um salário mínimo 39,4%) e em sua maioria de um à três salários mínimos (43,9%). Visto que os dados levantados não consideram aspectos subjetivos relacionados à local de origem e habitação bem como fonte de renda, não há como se inferir sobre a ligação com o uso de tecnologias, visto que não foi alvo do estudo. Esperava-se apenas verificar a percepção dos respondentes quanto ao acesso e disseminação de conteúdos que poderiam ser originários de *deepfake.*

Gráfico 5: Utilizo ou Já utilizei recomendações de filmes/músicas (Ex. netflix, spotify...).



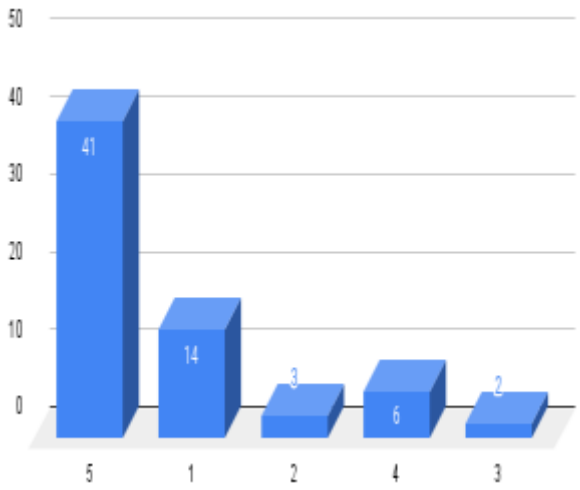
Fonte: Dados da Pesquisa (2024).

Gráfico 6: Utilizo ou Já utilizei assistentes virtuais, como Siri, Alexa...



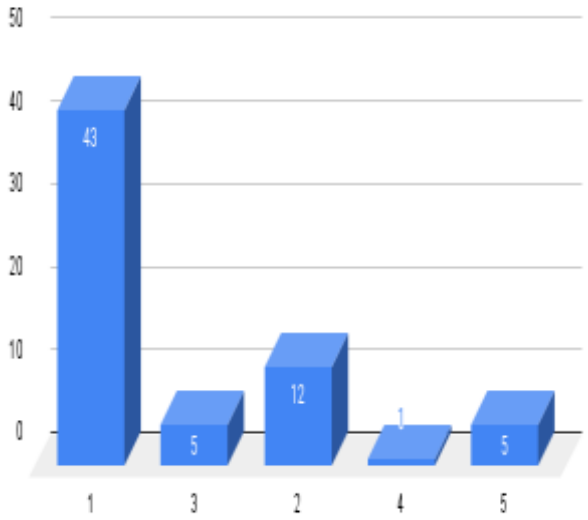
Fonte: Dados da Pesquisa (2024).

Gráfico 7: Utilizo ou já utilizei ferramenta de reconhecimento facial para desbloqueio de telefone



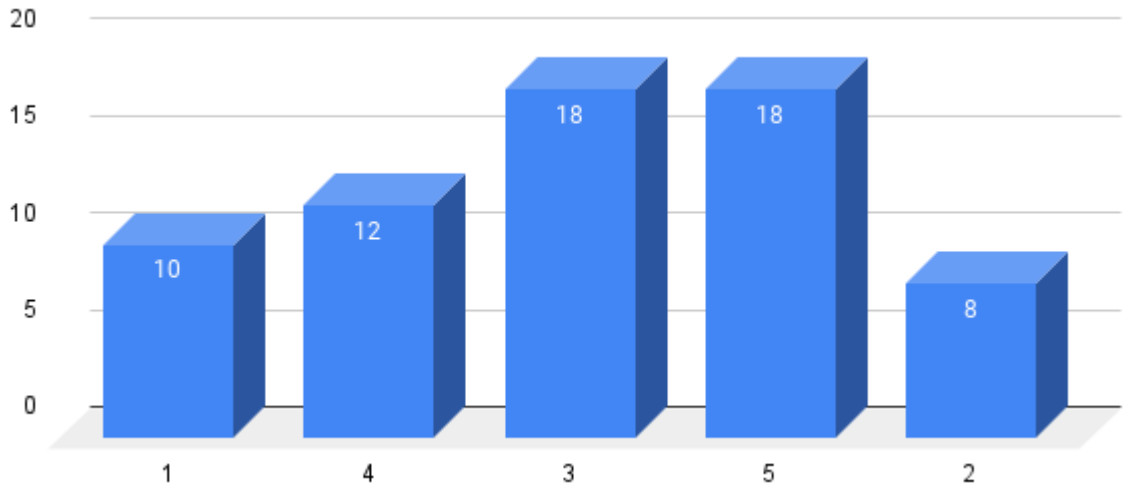
Fonte: Dados da Pesquisa (2024).

Gráfico 8: Utilizo ou já utilizei assistentes de escrita (ex: Grammarly)



Fonte: Dados da Pesquisa (2024).

Gráfico 9: Já criei, utilizei ou compartilhei algum meme, imagem ou vídeo que possa ter sido criado por meio de inteligência artificial



Fonte: Dados da Pesquisa (2024).

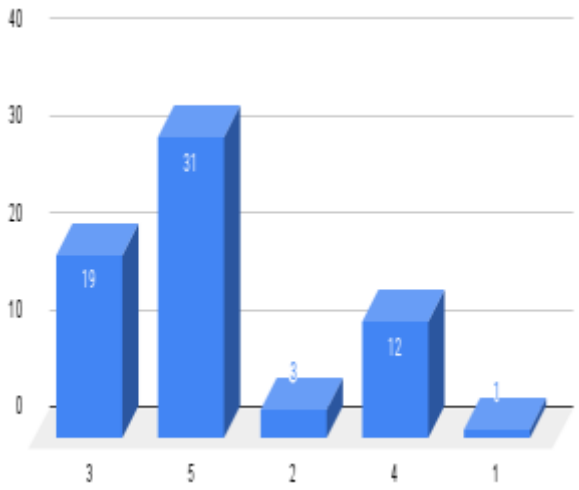
No tocante à categoria “utilização de material oriundo de inteligência artificial”, observa-se que 70% dos participantes destacam que é “muito frequente” o uso de recomendações de filmes/músicas (Ex. netflix, spotify...), corroborando o que Friedman (2007)

destaca quanto ao avanço tecnológico e o empoderamento dos indivíduos em meio à nova globalização. Por outro lado, observa-se o progresso contínuo citado por Kai Fu Lee, ao se observar que no tocante à utilização de assistentes virtuais, como Siri, Alexa, 20% dos respondentes “nunca” utilizou os assistentes virtuais que são cada vez mais comuns no cenário vigente.

No tocante à Utilização de ferramenta de reconhecimento facial para desbloqueio de telefone 68% destacam “muito frequente” e 10% “frequentemente” em contraponto à 23% que “nunca” utilizam ou utilizaram. 71,66% citam que nunca utilizam ou utilizaram assistentes de escrita (ex: Grammarly). O dado apresentado nesses dois gráficos pode refletir o que foi citado pela CNN (2023) quanto ao uso de smartphones como ferramenta de comunicação, amplamente utilizados.

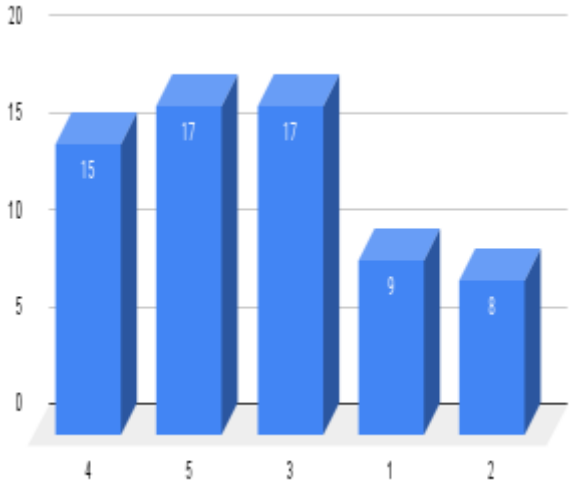
Quanto à criação, utilização ou compartilhamento de algum meme, imagem ou vídeo que possa ter sido criado por meio de inteligência artificial, destaca-se que os participantes reconhecem uma intensa utilização desse aspecto, com 30% “muito frequente”, 20% “frequente” e 30% “ocasionalmente”, reafirmando que a inteligência artificial (IA) está se fazendo cada vez mais presente na vida em sociedade, retratando a tamanha modernidade nos tempos atuais, e com isso, realidades nunca antes vivenciadas (LEE, 2019).

Gráfico 10: Inteligência Artificial (IA) é um ramo da ciência da computação que se concentra no **desenvolvimento de sistemas e algoritmos** capazes de realizar tarefas que normalmente exigem **inteligência humana**.



Fonte: Dados da Pesquisa (2024).

Gráfico 11: IAs são projetadas para realizar tarefas específicas e limitadas, como reconhecimento de voz, análise de dados, tradução automática ou recomendação de produtos.

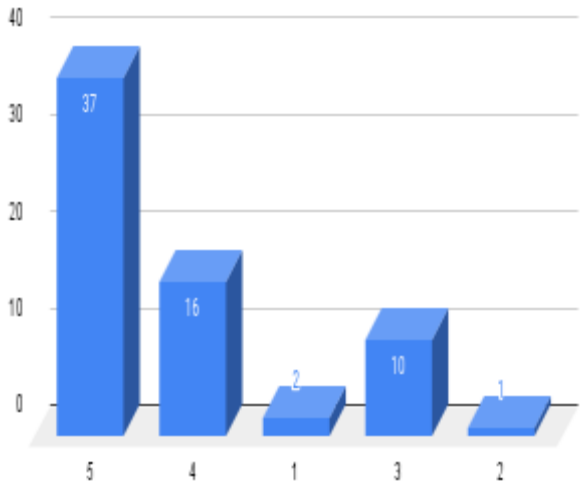


Fonte: Dados da Pesquisa (2024).

A segunda categoria analisada reflete o “conhecimento dos participantes acerca do que se trata a Inteligência Artificial e o fenômeno *deepfake”*. 51,66% “concorda totalmente” e 20% “concorda” que “Inteligência Artificial (IA) é um ramo da ciência da computação que se concentra no **desenvolvimento de sistemas e algoritmos** capazes de realizar tarefas que normalmente exigem **inteligência humana**” corroborando o conhecimento necessário à utilização do fenômeno o qual se estão vivenciando. Porém, o dado importante é o fato que 31,66% dos participantes não terem certeza quanto à afirmação “não estou decidido”, considerando provavelmente o destaque para as palavras “desenvolvimento de sistemas” e “inteligência humana” associada à inteligência artificial.

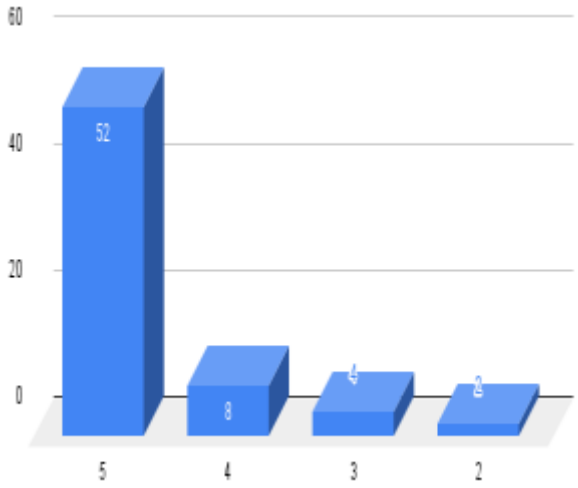
Por outro lado, o gráfico seguinte aponta incongruência quando a maioria 28,33% “concordo totalmente”, 25% “concordo” e 28,33% “nem concordo e nem discordo” que IAs são projetadas para realizar tarefas **específicas e limitadas**, como reconhecimento de voz, análise de dados, tradução automática ou recomendação de produtos.

Gráfico 12: *Deepfake* é uma **técnica que permite alterar um vídeo ou foto** com ajuda de inteligência artificial (IA).



Fonte: Dados da Pesquisa (2024)

Gráfico 13: Um dos usos mais preocupantes dessas ferramentas é a criação de vídeos com o rosto de outras pessoas, violando o direito de imagem.

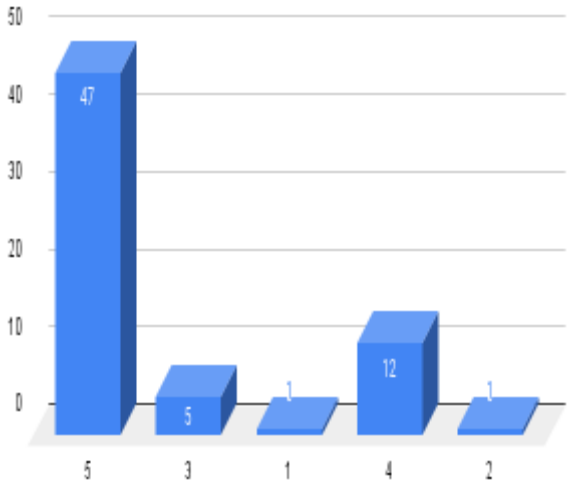


Fonte: Dados da Pesquisa (2024).

Os dados dos gráficos 12 e 13 apontam conhecem o fenômeno deepfake, pois 61,66% “concordam totalmente” e 26,66 “concordam” que d*eepfake* é uma **técnica que permite**

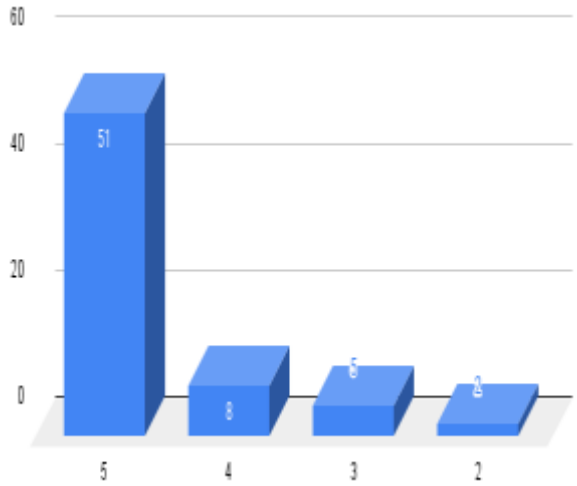
alterar um vídeo ou foto com ajuda de inteligência artificial (IA) trazendo à tona a preocupação de Russel (2021) quanto às possibilidades do uso de *deepfake*. Um dos usos mais preocupantes dessas ferramentas é a criação de vídeos com o rosto de outras pessoas, violando o direito de imagem, citados por Schreiber (2013), 86,66% "concorda totalmente" e 13,33% "concordam".

Gráfico 14: Deefakes podem representar riscos ao regime governamental, por exemplo em períodos eleitorais.



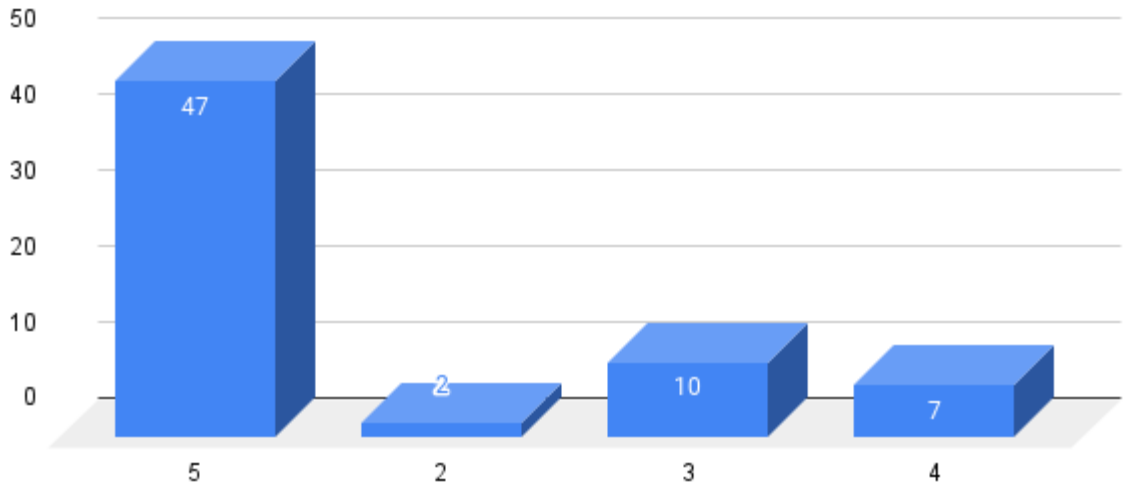
Fonte: Dados da Pesquisa (2024).

Gráfico 15: O Brasil precisa de leis específicas para regular o uso de *deepfake*, protegendo o direito de imagem.



Fonte: Dados da Pesquisa (2024).

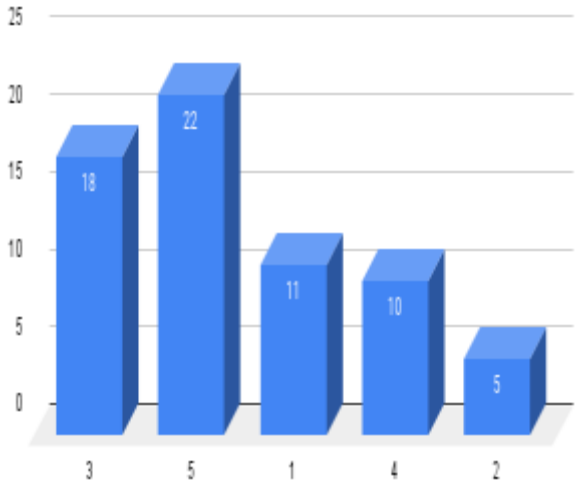
Gráfico 16: As plataformas online devem ser responsabilizadas, identificar e remover *deepfake*s.



Fonte: Dados da Pesquisa (2024)

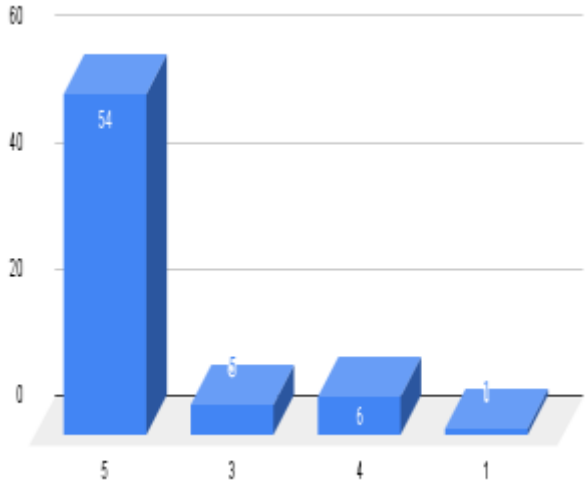
Na categoria Risco e Responsabilização” os dados mostram que 78,33% “concordam totalmente” que deefakes podem representar riscos ao regime governamental, por exemplo em períodos eleitorais. 85% “concordam totalmente” que o Brasil precisa de leis específicas para regular o uso de *deepfake*, protegendo o direito de imagem e 78,33% “concordam totalmente” que as plataformas online devem ser responsabilizadas, identificar e remover *deepfake*s.

Gráfico 17: O uso de *deepfake*s pode ser aceitável em alguns casos, como em produção de entretenimento.



Fonte: Dados da Pesquisa (2024).

Gráfico 18: Uma notícia falsa, por mais ingênua que possa parecer, é sempre prejudicial, pois induz ao erro e contribui para a desinformação da população, contribuindo para aumentar o cyberbullying e até questões mais drásticas associadas à vitima.



Fonte: Dados da Pesquisa (2024).

Um aspecto interessante na coleta de dados é que 90% dos participantes “concordam totalmente” que uma notícia falsa, por mais ingênua que possa parecer, é sempre prejudicial, pois induz ao erro e contribui para a desinformação da população, contribuindo para aumentar o cyberbullying e até questões mais drásticas associadas à vítima. Porém, se observa que há uma dúvida no tocante ao fato de que o uso de *deepfake*s pode ser aceitável em alguns casos, como em produção de entretenimento, quando apenas 13,2% destaca sua concordância. E é importante reforçar o que se destaca o art 5°, inc. X da CF/1988 quanto ao direito de personalidade.

Gráfico 19: A dificuldade em identificar ***deepfake*s** é amplificada quando consideramos a confiança natural que as pessoas depositam no que veem, especialmente quando o conteúdo é visualizado em telas pequenas, como as de smartphones, que podem obscurecer detalhes cruciais para a identificação de manipulações.

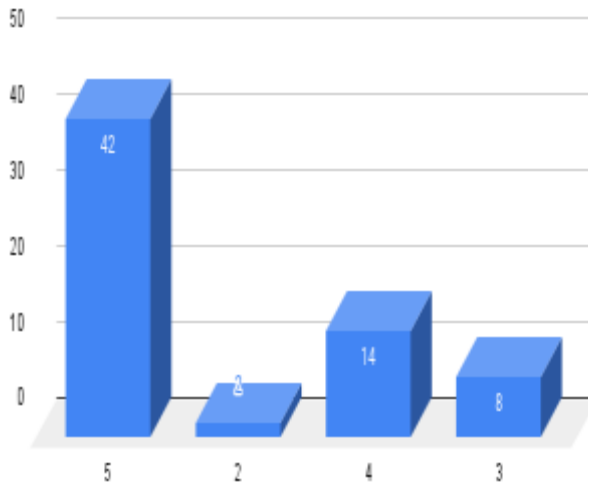
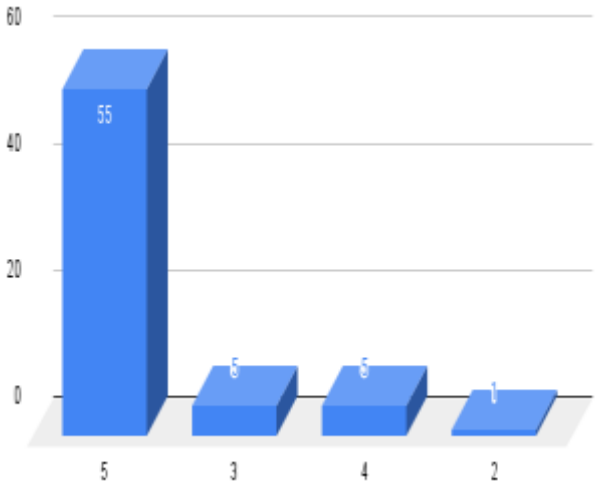


Gráfico 20: *Deepfake*s podem representar uma **ameaça** à privacidade e à segurança de empresas e indivíduos, além de serem usadas para diversos fins maliciosos, incluindo golpes de phishing, roubo de identidade e ataques automatizados de desinformação como fake news.

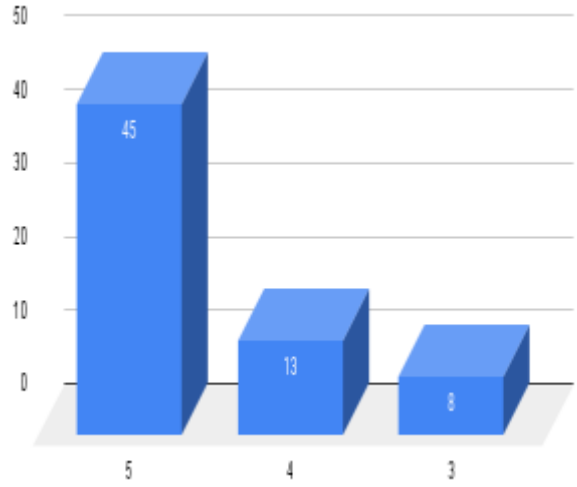


Fonte: Dados da Pesquisa (2024).

Fonte: Dados da Pesquisa (2024).

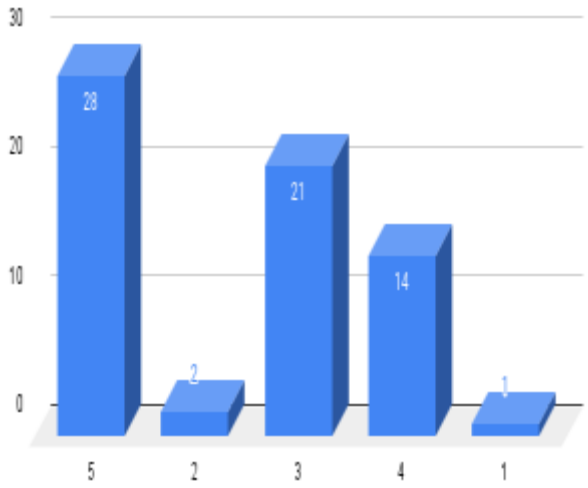
Observa-se que 70% “concorda totalmente” que a dificuldade em identificar ***deepfake*s** é amplificada quando consideramos a confiança natural que as pessoas depositam no que veem e 91,66% “concordam totalmente” que d*eepfake*s podem representar uma **ameaça** à privacidade e à segurança de empresas e indivíduos, além de serem usadas para diversos fins maliciosos, demonstrando mais uma vez um certo conhecimento e compreensão acerca dos riscos apresentados pelo fenômeno em pauta (JURID, 2023).

Gráfico 21: A violação à imagem da pessoa humana se traduz em todo e qualquer ato abusivo, desde a captação sem autorização (fotografia ou filme, por exemplo), até a sua forma de uso, protegido pelo artigo 5o, inciso X da Constituição Federal e pelo código civil.



Fonte: Dados da Pesquisa (2024).

Gráfico 22: A pena prevista pela violação ao direito de imagem é de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.



Fonte: Dados da Pesquisa (2024).

Cerca de 75% e 21,66% concordam que a violação à imagem da pessoa humana se traduz em todo e qualquer ato abusivo, desde a captação sem autorização (fotografia ou filme, por exemplo), até a sua forma de uso, protegido pelo artigo 5o, inciso X da Constituição Federal e pelo código civil. Mas observa-se que boa parte das pessoas não tem conhecimento de que o deepfake é um cibercrime 35% “Não esta decidido”, 3% “discorda” e 2% “discorda totalmente” quanto a entender que a pena prevista pela violação ao direito de imagem é de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro.

5 CONSIDERAÇÕES FINAIS

A inteligência artificial tem ajudado a tecnologia a ficar mais sofisticada e capaz de fazer tarefas complexas. Isso tem ajudado muitas áreas da sociedade a se tornarem mais eficientes e com mais qualidade de vida. Por outro lado, a partir do uso da IA, surge o Deepfake, que é uma forma de fazer vídeos falsos usando imagens e vídeos que já existem. Utilizam-se algoritmos

para ver padrões complexos em imagens. Permite criar situações irreais com imagens, vídeos e áudios, a partir do *deep lerning*, aprendizado profundo de máquina.

Os *deepfakes* podem prejudicar muitos aspectos da sociedade. Podendo-se criar e disseminar informações falsas, manipulando a opinião de usuários, causando a perda da confiabilidade de mídias digitais, tornando mais difícil identificar o que é real e o que é falso. A criação de vídeos ou imagens podem difamar ou caluniar alguém, causando danos irreparáveis à reputação da pessoa afetada.

Tendo em vista o objetivo geral de analisar a percepção de pessoas do Juazeiro do Norte-CE *deepfakes.* observa-se que o público investigado não apenas utiliza-se de tecnologia como de ferramentas que se utilizam de inteligência artificial, como conhecem e compreendem o fenômeno *deepfake*, porém se percebe que a compreensão acerca dos riscos, regulamentação e pena ainda deixam a desejar, o que deixa brechas para utilizações indevidas.

O Brasil ainda é carente de regulamentação devida e ampla disseminação quanto à importância e riscos do uso indiscriminado de ferramentas tecnológicas sem que haja uma educação pautada em princípios e leis que resguardem os usuários de tais mecanismos.

Em uma sociedade onde muitas informações são trocadas, o direito à privacidade é mais do que proteger a vida íntima. É o direito de manter o controle sobre os seus dados pessoais, a intimidade doméstica, características físicas, código genético, estado de saúde, crença religiosa, o fornecimento de dados de forma aparentemente sutil e inofensiva, ou qualquer outra informação pertinente à pessoa. A utilização de informações erradas, bem como a invasão de privacidade pode causar danos materiais ou morais.

É importante regulamentar a inteligência artificial com base em princípios éticos, morais e legais, para garantir que as pessoas possam usar a inteligência artificial de forma segura e confiável. Esses temas mostram a importância de considerar aspectos éticos e regulatórios para que a tecnologia seja desenvolvida e aplicada de maneira ética, responsável e benéfica para a sociedade, bem como o direito de personalidade.

O estudo em questão, dada a limitação no número de participantes, mostra-se apenas como um breve panorama acerca do cenário vivenciado. Os dados não são exaustivos, restando assim a possibilidade de exploração da lacuna legislativa, bem como estudos que explorem o fenômeno em profundidade e com abordagem qualitativa.

REFERÊNCIAS

ARRUDA, Cíntia da Silva. **Os avanços tecnológicos e a nova globalização**. 2019.

CANALTECH, **96% dos *deepfake*s são pornográficos, segundo relatório**. Disponível em: <https://canaltech.com.br/internet/96-dos-*deepfake*s-sao-pornograficos-segundo-relatorio-151749/> Acesso em: 31 mai. 2024.

COZMAN, Fabio G.; PLONSKI, Guilherme Ary; NERI, Hugo**. Inteligência artificial: avanços e tendências**. Universidade de São Paulo. Instituto de Estudos Avançados, 2021. Disponível em: <www.livrosabertos.abcd.usp.br/portaldelivrosUSP/catalog/book/650> Acesso em 31 mai. 2024.

CNN Brasil. **Saiba o que é *deepfake*, técnica de inteligência artificial que foi apropriada para produzir desinformação**. 2022. Disponível em: <https://www.cnnbrasil.com.br/noticias/saiba-o-que-e-*deepfake*-tecnica-de-inteligencia-artificial-que-foi-apropriada-para-produzir-desinformacao/> Acesso em: 29 mai. 2024.

CNN, **Novas tecnologias: tendência e o que esperar para o futuro**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/novas-tecnologias/> Acesso em: 31 mai. 2024.

DE BARROS, Rodrigo Monteiro. **Desafios Legais no Combate aos Crimes Cibernéticos:** uma Análise Jurídica. 2024. Disponível em: https://www.jusbrasil.com.br/artigos/desafios-legais-no-combate-aos-crimes-ciberneticos-uma-analise-juridica/2181538097 Acesso em 31 maio. 2024.

DE CASTRO BARBOSA, Xênia. **Breve introdução à história da Inteligência Artificial**. Jamaxi, v. 4, n. 1, 2020.

DE CASTRO SCHREIBER, Fernando Cesar; ANTUNES, Maria Cristina. **Cyberbullying: do virtual ao psicológico.** Boletim Academia Paulista de Psicologia, v. 35, n. 88, p. 109-125, 2015.

DENZIN, N. K. e LINCOLN, Y. S. Introdução: a disciplina e a prática da pesquisa qualitativa. In: DENZIN, N. K. e LINCOLN, Y. S. (Orgs.). **O planejamento da pesquisa qualitativa: teorias e abordagens**. 2. ed. Porto Alegre: Artmed, 2006.

***Deepfake*s**: ética e (ab)uso na era da inteligência artificial. Migalhas, 2024. Disponível em: https://lbca.com.br/*deepfake*s-etica-e-abuso-na-era-da-inteligencia-artificial/. Acesso em: 13 mai. 2024.

DLIPBLOG, **O que é inteligência artificial? Conceito, benefícios e mais**. Disponível em:<https://www.blip.ai/blog/tecnologia/inteligencia-artificial/#:~:text=O%20termo%20'Intelig%C3%AAncia%20Artificial'%20surgiu,de%20matem%C3%A1tica%20do%20Dartmouth%20College.>

EXAME, **Inteligência Artificial:** o que é e como funciona. Disponível em: <https://exame.com/inteligencia-artificial/inteligencia-artificial-o-que-e-e-como-funciona/>

FIA BUSINESS SCHOOL. **Crimes cibernéticos:** o que são, tipos, como detectar e se proteger. 2021. Disponível em: < https://fia.com.br/blog/crimes-ciberneticos/> Acesso em: 31 maio. 2024.

FOWLER JUNIOR, Floyd J. **Pesquisa de levantamento**. Tradução: Rafael Padilla Ferreira. Porto Alegre: Penso, 2011.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2018.

IBM, O que é inteligência artificial? Disponível em: <https://www.ibm.com/br-pt/topics/artificial-intelligence> Acesso em: 31 maio. 2024.

JORNAL JURID, **Como os avanços tecnológicos estão afetando a privacidade e a segurança dos dados dos cidadãos.** Disponível em:<https://www.jornaljurid.com.br/blog/auxilium/como-os-avancos-tecnologicos-estao-afetando-a-privacidade-e-a-seguranca-dos-dados-dos-cidadaos>

KASPERSKY, **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos.** Disponível em:<https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>

KAUFMAN. **A inteligência artificial irá suplantar a inteligência humana?** Edição. Estação das Letras e Cores. 2019.

LOURENÇO, Luciano**. Inteligência Artificial:** o que é e quais suas tecnologias. 2022. Disponível em: < https://latinoware.org/inteligencia-artificial-o-que-e-e-tecnologias/> Acesso em: 31 maio. 2024.

MIGALHAS, **A inteligência artificial e os limites no uso do direito de imagem.** Disponível em: <https://www.migalhas.com.br/depeso/390067/a-inteligencia-artificial-e-os-limites-no-uso-do-direito-de-imagem>

MIGALHAS, **Ética, privacidade e novas tecnologias:** o impacto da lei de proteção de dados na sociedade. Disponível em:https://www.migalhas.com.br/depeso/311142/etica--privacidade-e-novas-tecnologias--o-impacto-da-lei-de-protecao-de-dados-na-sociedade

MOSCO, Thays. **O que é Inteligência Artificial?** NEUROFEEDBACK, 2024. Disponível em: https://thaysmosko.com.br/glossario/o-que-e-inteligencia-artificial/. Acesso em 28 maio. 2024.

MPF, **Lei Geral de Proteção de Dados**. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd Acesso em: 31 mai. 2024.

NOAH, Yuval. **Sapiens:** Uma breve história da humanidade. Edição. L&PM. 2014

OLHAR, *Deepfake* de voz**: como a IA engana até 73% das pessoas**. Disponível em: <https://olhardigital.com.br/2023/08/03/seguranca/estudo-mostra-que-*deepfake*s-de-voz-ja-passam-batido-pelas-pessoas/>

ORIGEM, Qual a origem da tecnologia? Disponível em: <https://origemdascoisas.com.br/origem-da-tecnologia/

O que é ataque de DDos? Cloudfare, 2024. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/. Acesso em: 28 de maio. 2024.

PEREIRA, Verônica Aparecida; e ANDRADE, Rogério de. **Aspectos legais e motivacionais da adoção**. In. PEREIRA, Verônica Aparecida (ORG.). Parentalidade adotiva: diálogos e reflexões. 1.ed. Curitiba, Brazil Publishing, 2021.

RAPADURA TECH, **O impacto dos *deepfake*s na sociedade:** da diversão à desinformação. Disponível em:<https://rapaduratech.com.br/*deepfake*s-revolucao-digital-e-os-desafios/>

RUSSEL, Norving. **Inteligência artificial.** Edição. CAMPUS. 2013

RUSSEL, Norving. **Inteligência artificial a nosso favor:** como manter o controle sobre a tecnologia. Edição. Companhia das letras. 2021.

SCHREIBER, Anderson. Direitos da personalidade, 2° Edição, ATLAS,2013.

SOUZA, Victor**. Inteligência Artificial:** O *deepfake* e seus impactos no direito da personalidade, á luz do direito brasileiro. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/15650> Acesso em: 31 mai. 2024.

Studio ESTRATÉGIA. **IA:** Inteligência Artificial e a Revolução da Gestão Financeira e Estratégia nos Negócios, 2019. Disponível em: <https://studioestrategia.com.br/inteligencia-artificial-e-gestao-financeira/> Acesso em: 29 maio. 2024

TEFFÉ, Chiara Spadaccini de. Considerações sobre a proteção do direito à imagem na internet. **Revista de Informação Legislativa**, Brasília, a. 54 n. 213, jan./mar. 2017 p. 173-198.

TOMASEVICIUS FILHO, Eduardo. **Inteligência artificial e direitos da personalidade**: uma contradição em termos? Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/156553/152042>

ZERUM. **Espionagem cibernética:** A ameaça silenciosa, 2023. Disponível em: <https://www.zerum.com/pt/cybersecurity/espionagem-cibernetica-a-ameaca-silenciosa/#:~:text=O%20que%20%C3%A9%20espionagem%20cibern%C3%A9tica,velado%20dentro%20dos%20sistemas%20invadidos> Acesso em: 29 maio. 2024.