FACULDADE SANTÍSSIMO SACRAMENTO
CURSO DE BACHARELADO EM DIREITO

MÁRLON CARDOSO DOS SANTOS

POR VERDADES VIRTUAIS: *DEEPFAKE*, FAKE NEWS E A RESPONSABILIDADE JURÍDICA NO CENÁRIO LEGAL BRASILEIRO

Alagoinhas-BA
2023

MÁRLON CARDOSO DOS SANTOS

POR VERDADES VIRTUAIS: *DEEPFAKE*, FAKE NEWS E A RESPONSABILIDADE JURÍDICA NO CENÁRIO LEGAL BRASILEIRO

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do título de Bacharel em Direito da Faculdade Santíssimo Sacramento.

Orientador (a): Prof. Me. Marjorie da Silva Ribeiro Souza.

Alagoinhas-BA
2023

MÁRLON CARDOSO DOS SANTOS

POR VERDADES VIRTUAIS: *DEEPFAKE*, FAKE NEWS E A RESPONSABILIDADE JURÍDICA NO CENÁRIO LEGAL BRASILEIRO

Trabalho de Conclusão de Curso, aprovado como requisito para obtenção de título de Bacharel em Direito da Faculdade Santíssimo Sacramento

Data de Aprovação

___/___/____

BANCA EXAMINADORA

_____

Prof. Dr./Dra. ou Me./Ma. ou Esp. Marjorie da Silva Ribeiro Souza
Faculdade Santíssimo Sacramento

_____

Prof. Dr./Dra. ou Me./Ma. ou Esp. Leandro Carvalho Sanson
Faculdade Santíssimo Sacramento

_____

Prof. Dr./Dra. ou Me./Ma. ou Esp. Tuany Sande Cardoso
Faculdade Santíssimo Sacramento

AGRADECIMENTOS

Durante nossa trajetória, cruzamos caminhos com indivíduos extraordinários. São aqueles que não só nos motivam a crescer, mas também nos desafiam a sonhar e nos dão um propósito maior além da simples existência. Eles se tornam os pilares que sustentam nossos voos mais altos, nos conduzindo a alcançar metas que jamais imaginávamos serem possíveis.

Agradeço especialmente a Marjorie da Silva Ribeiro Souza e Marcio Santos da Conceição, cujo apoio e orientação foram fundamentais para esta trajetória. As suas palavras de incentivo e sabedoria brilharam como faróis nos momentos mais desafiadores, apontando-nos para novos caminhos a seguir.

À minha família, pelo amor incondicional e apoio constante, agradeço por serem minha fonte de força e inspiração. Cada gesto e palavra de incentivo moldaram esta jornada de forma indelével. Aos meus amigos e colegas de curso, pelo apoio mútuo, troca de experiências e momentos compartilhados, que tornaram essa jornada acadêmica mais enriquecedora e prazerosa.

Agradeço também a todos os professores, funcionários e profissionais que, de alguma forma, contribuíram para o desenvolvimento deste trabalho, em especial ao Coordenador Leandro Carvalho Sanson por seu apoio e ensinamentos ao longo dos anos.

Por fim, dedico um agradecimento especial a todas as fontes, autores e instituições cujos trabalhos foram referenciados e que enriqueceram este estudo com seu conhecimento.

A todos vocês, que deram cor, significado e impulso a esta jornada, meu mais profundo obrigado.

RESUMO

No cenário da democratização da informação por meio das mídias digitais, o fenômeno da *deepfake* e da fake news levanta sérias preocupações em relação à responsabilidade jurídica, abarcando da esfera cível à criminal. Nessa perspectiva, o presente trabalho busca responder ao seguinte problema de pesquisa: De que maneira a criação e disseminação de fake news, principalmente como o emprego de tecnologia *deepfake*, impacta na possibilidade de responsabilização dentro do ordenamento jurídico brasileiro? O objetivo geral do trabalho é analisar de que forma a utilização de deepfake, através de fake news, se configura como uma ferramenta poderosa para a disseminação de informações fraudulentas, com foco na possibilidade de responsabilização do agente, abrangendo tanto a esfera cível quanto a criminal, como meio de combater esse fenômeno e suas potenciais consequências. A pesquisa em questão é caracterizada como qualitativa, adotando o método dedutivo e iniciando com uma fase exploratória. Para embasar o estudo, foi conduzida uma pesquisa bibliográfica, consultando livros e artigos científicos que abordam a temática escolhida, por meio de três objetivos específicos: O primeiro visa examinar a natureza da informação e desinformação na era pós-moderna, das redes sociais e das fake news na sociedade, bem como da tecnologia de *deepfake* e sua conexão intrínseca com a disseminação de notícias falsas; O segundo avaliar como o direito à informação é protegido na legislação brasileira e a responsabilização das plataformas on-line que disseminam conteúdo desinformativo; E o terceiro, destacar a intervenção do direito penal como uma das maneiras de proteger o direito à informação, abordando os crimes que podem surgir da produção e disseminação de notícias fraudulentas, especialmente quando envolve o uso de *deepfake* no contexto brasileiro. Sob essa ótica, ao debruçar-se sobre os aspectos jurídicos que a produção e compartilhamento de notícias falsas na internet propiciam, conclui-se que, embora haja possibilidade de responsabilização tanto civil quanto criminal, é crucial que o Poder Legislativo e Judiciário intervenham de maneira decisiva nessas questões. A inação pode gerar na sociedade a percepção de ausência de normas efetivas para combater a propagação de desinformação, comprometendo a efetividade das medidas preventivas estabelecidas.

Palavras-chave: *Deepfake*. Fake news. Responsabilidade Criminal-Cível.

ABSTRACT

In the scenario of democratization of information through digital media, the phenomenon of deepfake and fake news raises serious concerns in relation to legal responsibility, ranging from civil to criminal spheres. From this perspective, this work seeks to answer the following research problem: How does the creation and dissemination of fake news, especially the use of deepfake technology, impact the possibility of accountability within the Brazilian legal system? The general objective of the work is to analyze how the use of deepfake, through fake news, is a powerful tool for the dissemination of fraudulent information, focusing on the possibility of holding the agent accountable, covering both the civil and criminal spheres. , as a means of combating this phenomenon and its potential consequences. The research in question is characterized as qualitative, adopting the deductive method and starting with an exploratory phase. To support the study, a bibliographical research was conducted, consulting books and scientific articles that address the chosen theme, through three specific objectives: The first aims to examine the nature of information and disinformation in the post-modern era, social networks and fake news in society, as well as deepfake technology and its intrinsic connection with the dissemination of fake news; The second evaluates how the right to information is protected in Brazilian legislation and the accountability of online platforms that disseminate disinformative content; And the third, highlighting the intervention of criminal law as one of the ways to protect the right to information, addressing crimes that may arise from the production and dissemination of fraudulent news, especially when it involves the use of deepfake in the Brazilian context. From this perspective, when looking at the legal aspects that the production and sharing of fake news on the internet provides, it is concluded that, although there is the possibility of both civil and criminal liability, it is crucial that the Legislative and Judiciary branches intervene in a manner decisive on these issues. Inaction can generate in society the perception of a lack of effective standards to combat the spread of misinformation, compromising the effectiveness of established preventive measures.

Keywords: Deepfake. Criminal-Civil Liability. Fake news.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

A era da informação digitalizada e amplamente acessível trouxe consigo uma série de avanços e desafios para a sociedade contemporânea. Entre esses desafios, destacam-se a disseminação de notícias falsas e a manipulação de mídia, fenômenos que têm encontrado na tecnologia de *deepfake* um aliado poderoso. Neste contexto, a presente pesquisa busca analisar como esse evento tem sido tratado no âmbito do ordenamento jurídico brasileiro, positivado ou no âmbito legislativo, no intuito de verificar se tais instrumentos legais estão sendo suficientes à proteção do direito fundamental à informação.

A partir da crescente influência das redes sociais e das plataformas digitais na disseminação de informações, tornou-se imperativo compreender como a manipulação de mídia, por meio da tecnologia de *deepfake*, está interligada com a propagação de fake news. O uso dessas tecnologias tem o potencial de confundir o público, minar a confiabilidade das fontes de informação e afetar a estabilidade democrática.

Assim, ao longo deste trabalho, buscar-se-á lançar luz sobre a complexa interconexão entre *deepfake* e as fakes news, bem como seus desdobramentos no cenário jurídico, contribuindo para uma compreensão mais abrangente e crítica deste desafio contemporâneo. Partindo desse pressuposto, este trabalho tem como pergunta norteadora: De que maneira a criação e disseminação de fake news, principalmente como o emprego de tecnologia *deepfake*, impacta na possibilidade de responsabilização dentro do ordenamento jurídico brasileiro?

Por todo exposto acima, este trabalho monográfico tem como objetivo geral analisar de que forma a utilização de *deepfake*, através de fake news, se configura como uma ferramenta poderosa para a disseminação de informações fraudulentas, com foco na possibilidade de responsabilização do agente, abrangendo tanto a esfera cível quanto a criminal, como meio de combater esse fenômeno e suas potenciais consequências. E se estrutura sobre três objetivos específicos que, progressivamente, vão aprofundar tal análise.

No primeiro objetivo examina-se a natureza da informação e desinformação na era pós-moderna, das redes sociais e das fake news na sociedade, bem como da tecnologia de deepfake e sua conexão intrínseca com a disseminação de notícias falsas.

No segundo objetivo avalia-se como o direito à informação é protegido na legislação brasileira, discutindo desafios e debates em relação à responsabilização das plataformas on-line que veiculam conteúdo desinformativo. Além disso, buscar as ferramentas jurídicas

existentes para combater e prevenir a desinformação on-line, como o Marco Civil da Internet e o Projeto de Lei n. 2630/2020, conhecido como o PL das Fake news, e as implicações desse projeto para a proteção do direito à informação.

Por último, no terceiro objetivo destaca-se a intervenção do direito penal como uma das maneiras de proteger o direito à informação, abordando os crimes que podem surgir da produção e disseminação de notícias fraudulentas, especialmente quando envolve o uso de *deepfake* no contexto brasileiro.

A escolha deste tema é justificada pela necessidade premente de compreender os impactos resultantes da criação de deepfakes e da disseminação de notícias falsas. Essa compreensão é essencial para o desenvolvimento de estratégias eficazes no combate às potenciais transgressões previstas no ordenamento jurídico nacional. Além disso, destaca-se a urgência em evidenciar as ameaças à integridade da informação e à reputação de indivíduos e instituições, ressaltando também a potencial influência dessas práticas sobre a estabilidade democrática. Nesse contexto, aprofundar-se nessa relação torna-se imperativo não apenas para compreender as consequências imediatas, mas também para propor aprimoramentos legislativos, judiciários e políticas públicas capazes de enfrentar os desafios emergentes decorrentes dos avanços tecnológicos.

A abordagem metodológica deste estudo se baseou em uma revisão abrangente de fontes bibliográficas, incluindo livros, artigos e periódicos relacionados ao tópico em análise, bem como literatura jurídico-científica pertinente. Este trabalho é caracterizado como um método dedutivo e abordagem qualitativa, uma vez que estrutura-se sobre um raciocínio lógico com a finalidade de se chegar a uma conclusão específica.

Outrossim, é, em essência, uma revisão de literatura que explora os principais fatores relacionados a notícias falsas, manipulação de mídia e a possível responsabilidade penal. Ele considera as ideias dos autores apresentados e segue uma estrutura que inclui introdução, capítulos relevantes ao tema, conclusão e referências bibliográficas.

1 A INFORMAÇÃO E A DESINFORMAÇÃO NA ERA PÓS MODERNA

Na era pós-moderna, a informação e a desinformação tornaram-se temas de extrema relevância. Com o avanço da tecnologia e a popularização da internet, a sociedade passou a ter acesso cada vez mais fácil e rápido às informações. Em contrapartida, surgiram também os problemas da desinformação, como exemplo disso temos a disseminação de notícias falsas e a manipulação de conteúdos de mídia, que geram impactos significativos na sociedade, afetando a opinião pública, eleições, a reputação de pessoas e instituições, bem como a convivência democrática.

Neste capítulo será abordada a importância da informação e da desinformação na era pós-moderna, como o conceito de tecnologia, internet e Tecnologia da Informação e Comunicação (TIC), bem como a influência das redes sociais e plataformas tecnológicas. Pretende-se explorar o fenômeno das fake news, abordando o conceito, tipologias e exemplos históricos. Ao final do capítulo, será destacado a preocupação com as *deepfakes*, uma forma avançada de manipulação de conteúdo, e sua relação com notícias falsas.

1.1 CONCEITUANDO A TECNOLOGIA, INTERNET E TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC

A tecnologia desempenha um papel fundamental na sociedade contemporânea, impulsionando o progresso e a inovação em áreas como comunicação, medicina, indústria e pesquisa. Seu constante avanço molda o mundo em constante evolução em que se vive. De acordo com Waldimir Longo (1984), a tecnologia abrange um conjunto de conhecimentos científicos ou empíricos aplicados na produção e comercialização de bens e serviços, desempenhando um papel essencial na economia e na sociedade moderna. Por outro lado, Abetti (1989), citado por Steensma (1996), define a tecnologia como um conjunto de conhecimentos, ferramentas e técnicas oriundos da ciência e da experiência prática, utilizado no desenvolvimento, projeto, produção e aplicação de produtos, processos, sistemas e serviços.

Um exemplo marcante desse avanço tecnológico é o surgimento do computador, uma máquina que automatiza o processamento de uma ampla gama de dados e informações. Esse dispositivo resolveu inúmeros problemas e contribuiu para a elucidação de muitos outros (Cormen, 2012). No entanto, seu impacto nas mudanças sociais e na esfera pública seria mínimo, se considerado isoladamente. Foi com a chegada da internet que as ferramentas

computacionais transformaram de maneira revolucionária o cenário das comunicações sociais (Postman, 1993).

A palavra “internet”, que surgiu da fusão de duas palavras de origem inglesa, “*international network*” (rede internacional), pode ser conceituada como uma rede global de computadores interligados, possibilitando a transmissão de dados e informações para qualquer usuário conectado a ela (Eduvirges; Santos, 2013).

A internet se origina a partir de uma série de estudos e experimentos que objetivavam melhorar a interconexão de computadores, impulsionados por uma iniciativa governamental na década de 1960. A Agência de Projetos de Pesquisa Avançada de Defesa dos EUA (*Defense Advanced Research Projects Agency* - DARPA) colaborou com várias universidades e seus pesquisadores para criar uma rede de computadores chamada ARPANET. O propósito dessa rede era viabilizar a interação entre computadores, de modo que pesquisadores de diversas universidades pudessem compartilhar recursos de computação (Dantas, 2017).

Em 1989, o físico e pesquisador Timothy John Berners-Lee, considerado o pai da internet, criou a *World Wide Web*, o que comumente chama-se de web. O termo pode ser traduzido para o português como "rede de alcance mundial" e representa a plataforma fundamental para a popularização da internet, conforme a conhecemos hoje (Cintra, 2003).

> A web pode ser definida como um conjunto de recursos que possibilita navegar na Internet por meio de textos hipersensíveis com hiper-referências em forma de palavras, títulos, imagens ou fotos, ligando páginas de um mesmo computador ou de computadores diferentes. A web é o segmento que mais cresce na internet e a cada dia ocupa espaços de antigas interfaces da rede. (Vilha, 2002, p. 56)

Na perspectiva técnica, a internet representa uma ampla rede que interliga um grande número de computadores ao redor do mundo. Essas conexões são estabelecidas por meio de várias tecnologias, incluindo redes telefônicas, cabos e satélites. Assim, a rede telemática oferece oportunidades para encontros, interações, diálogos e o desenvolvimento de relações entre indivíduos, apresentando vantagens e desafios inerentes às interações sociais (Paesani, 2013).

A interconexão global provocada pela internet é potencializada pelas Tecnologias da Informação e Comunicação (TICs), o que tornou ferramentas fundamentais para disseminar informações e conectar usuários. As TICs englobam um conjunto completo de tecnologias que viabilizam a produção, acesso e disseminação de informações, além da comunicação entre pessoas. Com o avanço tecnológico, novas tecnologias surgiram e se difundiram

mundialmente, facilitando o compartilhamento de conhecimento e a comunicação entre pessoas, independentemente do lugar onde esteja (Rodrigues et al., 2014).

As Tecnologias da Informação e Comunicação (TICs) encontram aplicação em diversas áreas, como por exemplo na indústria, comércio e educação. Em todas essas áreas, o objetivo principal das TICs é proporcionar automação da informação e comunicação, o que abrange um conjunto de tecnologias emergentes, incluindo *softwares* e *hardwares*[1], que asseguram a funcionalidade da comunicação. A ampla popularização das TICs coincidiu com o advento e a disseminação da internet (Pacievitch, 2014). Assim, a popularização da internet foi desencadeada pelo uso extensivo das TICs, criando uma cooperação que transformou a forma como nos comunicamos e compartilhamos informações.

Irlla Diniz (2012) enfatiza que as Tecnologias da Informação e Comunicação (TICs) desempenham um papel considerável na vida cotidiana da população, ocupando um espaço importante no meio social. Dessa forma, as TICs, aliadas à internet, transformaram não apenas a comunicação, mas também a forma como acessa-se e compartilha-se informações em nossa sociedade contemporânea.

1.2 A TIC E O UNIVERSO DIGITAL: AS REDES SOCIAIS E AS PLATAFORMAS DE TECNOLOGIA

Com o advento da internet, emergem as redes sociais virtuais ou on-line, que são plataformas de comunicação em que qualquer indivíduo tem a oportunidade de se conectar com qualquer pessoa ao redor do mundo. Estas plataformas permitem a transmissão e recebimento de informações de forma instantânea e contínua. Não obstante, é perceptível que ocorre um desvio de propósito nas redes sociais, à medida que os usuários passam a compartilhar informações que invadem a esfera privada de terceiros, resultando em danos de várias naturezas (Carvalho, 2013).

Conforme destacado por Martha Gabriel (2010) em sua obra “Marketing na Era Digital”, as redes sociais digitais estão entre as formas de comunicação de maior crescimento e difusão em escala global, impactando comportamentos e relacionamentos de maneira significativa. A referida autora esclarece que uma rede social é uma estrutura composta por indivíduos ou empresas interconectados por diferentes tipos de vínculo, como amizade, parentesco, afinidade, transações financeiras, afinidades de crenças, intercâmbio de conhecimento, relações amorosas, entre outros. Assim, as redes representam uma reunião da

[1] O hardware representa a parte física do computador, enquanto o software é a parte lógica do computador.

sociedade, com o objetivo de conectar pessoas e facilitar a comunicação. No contexto da internet, as redes sociais são representadas por páginas da web que criam mecanismos para facilitar a interação entre seus membros, independentemente de sua localização.

> Se, por um lado, redes sociais relacionam-se a pessoas conectadas em função de um interesse em comum, mídias sociais associam-se a conteúdos (textos, imagem, vídeo etc.) gerados e compartilhados pelas pessoas nas redes sociais. Dessa forma, tanto redes sociais como mídias sociais, em sua essência, não tem nada a ver com tecnologia, mas com pessoas e conexões humanas. A tecnologia apenas facilita e favorece a interação das pessoas e a criação e compartilhamento de conteúdo por elas. Assim, as redes sociais, como o Facebook, por exemplo, são plataformas que possibilitam, facilitam e potencializam a conexão de pessoas com outras pessoas, ampliando o alcance das redes sociais pessoais, e ferramentas de armazenamento e compartilhamento que alavancam o volume de mídias sociais criadas pelas pessoas. Assim, um site de redes sociais on-line é apenas uma plataforma tecnológica que favorece a atuação das pessoas para interagir e compartilhar conteúdos em suas redes sociais. (Gabriel, 2010, p.202).

A utilização das redes sociais no mundo virtual é crucial, pois oferece uma diversidade de formas de relacionamento e uma abordagem horizontal, sem hierarquias, onde os membros compartilham informações, conhecimentos, objetivos comuns e interesses (Carvalho, 2013). No entanto, o século XXI é caracterizado pela ascensão de plataformas digitais que, por meio de seus algoritmos, exercem influência nas vidas das pessoas em diversos setores, sem fornecer informações claras sobre a coleta e o uso dos dados, evidenciando uma falta de transparência (Poell; Nieborg; Van Dijck, 2020, apud Grohmann, 2020).

Essas plataformas representam sistemas digitais complexos que possibilitam interações e transações entre diferentes grupos de usuários, sejam indivíduos, empresas, organizações ou dispositivos conectados. Elas funcionam como intermediários reunindo e conectando participantes interessados em trocar bens, serviços, informações ou experiências, transformando setores inteiros da economia e influenciando a forma como as pessoas vivem, trabalham e se relacionam (Parker; Altyne; Choudary, 2016). Esse novo momento na cultura digital, é conhecido como Plataformização, Dataficação e Performatividade Algorítmica (PDPA), e representa a convergência de elementos-chave na era digital, conforme a perspectiva de André Lemos (2020).

Em contrapartida, as plataformas digitais atualmente não são apenas inofensivas e imperceptíveis. São, também, poderosos blocos com interesses mercantis ocultos, lobistas e projetos de dominação global (Morozov, 2018), o que evidencia o impacto significativo que as plataformas digitais têm na sociedade contemporânea.

1.3 FAKE NEWS: CONCEITO, TIPOLOGIAS E EXEMPLOS HISTÓRICOS

Eleita a palavra do ano de 2017 pelo dicionário em inglês da editora britânica Collins (Bbc, 2017), a expressão fake news passou a ganhar notoriedade a partir do ano de 2016, no contexto da corrida presidencial norte-americana, quando ex-presidente Donald Trump utilizou amplamente o termo para se referir às notícias negativas que circulavam na internet sobre ele.

Ao conceituar a expressão "fake news", Renê Braga (2018) acentua que esta, se trata de notícias que são claramente falsas ou enganosas divulgadas por diferentes meios de comunicação, cuja finalidade do emissor é chamar a atenção para desinformar ou obter alguma vantagem (indevida) no âmbito social, político ou econômico.

Nesse contexto, é perceptível que as "fake news" têm o potencial de manipular grandes massas objetivando atingir movimentos ou resultados específicos, induzindo o leitor ao erro, bem como deteriorar informações verdadeiras, praticar infrações penais e propagar boatos que podem atingir a honra de diversas pessoas, principalmente de alvos políticos, conforme salienta Luis Bussular (2018).

Partindo desse pressuposto, pode-se definir fake news como informações de diferentes vertentes que são apresentadas como verídicas, contudo, são evidentemente falsas, fabricadas, ou ampliadas ao ponto de deixar de refletir a realidade; outrossim, a informação opera com a finalidade explícita de ludibriar ou confundir um alvo ou público específico (Reilly, 2018 apud Meneses, 2018). De forma mais resumida, fake news pode ser conceituada como informações deliberadamente e comprovadamente falsas, com potencial para enganar os leitores (Allcott, 2017).

1.3.1 Tipos de fake news

De acordo com a classificação de Claire Wardle (2017), é possível identificar sete categorias distintas de fake news. Cada uma com suas próprias características e implicações, a saber:

Sátira ou Paródia: Inclui conteúdos humorísticos e satíricos que podem ser confundidos como informações verdadeiras. Apesar de não ter a intenção de prejudicar, pode ter o potencial de induzir em erro.

Ademais, existe uma distinção entre as sátiras e paródias. Enquanto as sátiras imitam programas de notícias fictícias, geralmente incorporando elementos humorísticos ou exagerados, o objetivo é fornecer ao público atualizações fictícias de notícias. Nas paródias

são introduzidos no conteúdo elementos que carecem de fundamento factual, com a intenção de gerar um efeito humorístico, indo além do que é usualmente encontrado na sátira. Contudo, na paródia, a estrutura semelhante ao formato jornalístico é mais proeminente, o que pode levar a uma maior facilidade de confusão com eventos reais (Tandoc Jr. et al., 2017).

No cenário nacional, o Sensacionalista se destaca como um renomado exemplo de noticiário satírico e paródico. Seu slogan, habilmente brincando com as palavras, declara: "Um jornal isento de verdade".

Falsa Conexão: Isso ocorre quando as imagens, títulos ou legendas dão pistas falsas sobre o verdadeiro conteúdo, podendo levar a uma interpretação errônea. Cesar Gomes, em seu artigo intitulado "Os 7 tipos de Fake news sobre a Covid-19 (2020)", destacou que a "Falsa Conexão" de fato apresenta uma fonte aparentemente legítima, mas manipula o conteúdo proveniente dessa fonte. Isso muitas vezes se baseia na tendência comum das pessoas de não verificar a fonte por si mesmas, aceitando o que é apresentado na postagem como verdadeiro. Esse fenômeno está interligado a diversos fatores, como viés de confirmação e outros motivos que contribuem para a propagação de notícias falsas.

No dia 1º de abril de 2014, o site da NPR, uma organização de mídia que abrange notícias e produz programas de rádio, veiculou um artigo chamado "Por que a América não lê mais?" (Npr, 2014). Ao clicar no link da matéria, os leitores eram redirecionados para a página da NPR, onde eram instruídos apenas a curtir a postagem, sem deixar comentários. Muitos usuários comentaram sobre a publicação, demonstrando indignação com o título do artigo, indicando que certamente tais usuários não leram a notícia.

Conteúdo Enganoso: Envolve o uso de informações enganosas para prejudicar um assunto ou pessoa, deturpando a verdade. Segundo Gomes (on-line, 2020), "este tipo de desinformação não apresenta nenhuma fonte oficial e circula por meio de imagens e vídeos de perfis ligados a determinadas posições políticas".

Um exemplo disso ocorreu após o trágico assassinato da vereadora Marielle Franco no Rio de Janeiro, em março de 2018. Durante esse período, surgiram notícias afirmando que Marielle havia engravidado aos 16 anos, sido casada com Marcinho VP, um ex-traficante, e apoiadora do Comando Vermelho. No entanto, uma investigação do site Boatos.org, dedicado a desmascarar notícias falsas on-line, revelou que essas informações eram falsas. As *fakes news* sobre Marielle tinham uma agenda política, visando difamar e diminuir suas realizações e lutas (Almeida, 2018).

Falso Contexto: Compreende um conteúdo original com informações completamente inventadas, apresentadas como se fossem notícias reais, ou seja, o conteúdo original é compartilhado em um contexto alterado, distorcendo sua verdadeira intenção.

Uma espécie dessa ocorreu no ano de 2017, quando a Organização Internacional para Migrações das Nações Unidas expôs a existência de mercados de escravos na Líbia e Níger. Nestes mercados, centenas de jovens que buscavam migrar para a Líbia a partir de outras partes do continente africano estavam sendo submetidos a um comércio de compra e venda (Macguil, 2017).

Algum tempo depois, um indivíduo no Facebook com o nome de Rayon Pyne compartilhou várias fotos alegando que retratavam o tráfico de escravos na Líbia. No entanto, de acordo com o site de verificação de fatos Snopes (Macguil, 2017), das sete imagens postadas, apenas duas estavam de fato relacionadas ao tráfico, enquanto as outras cinco não possuíam qualquer conexão com o assunto. Além disso, as fontes das duas imagens restantes permaneceram sem identificação.

Conteúdo de Impostor: Nesse caso, afirmações falsas são atribuídas a fontes genuínas, frequentemente a pessoas reais. Embora não seja excluída a possibilidade de motivações político-partidárias, a categoria "Sátira ou Paródia", ao contrário de outros tipos de desinformação, não tem como intenção enganar, mas sim proporcionar entretenimento.

Manipulação de Conteúdo: Refere-se à edição ou manipulação de informações reais para criar uma narrativa enganosa. Um exemplo disso é a imagem que circulou pelas redes sociais, retratando o momento em que a rainha Elizabeth II supostamente nomeia um gato como cavaleiro da Ordem do Império Britânico. Entretanto, essa foto é uma montagem criada a partir de uma imagem genuína, capturada em 2019, quando a rainha realmente concedeu a honraria de Knight Bachelor do Império Britânico ao ator inglês Simon Russell Beale, durante uma cerimônia no Palácio de Buckingham (G1, 2022).

Figura 1: Rainha Elizabeth II dando título de cavaleiro a um gato. Fonte: (G1, 2022).

Vídeos editados intencionalmente em partes específicas também têm um impacto significativo na internet. Essa prática é frequente em discursos políticos, onde segmentos são escolhidos de modo a apresentar informações fora de contexto. Os cortes muitas vezes passam despercebidos pelos espectadores, resultando na disseminação ampliada de fake news. Além disso, existem softwares projetados para simplificar a manipulação de vídeos, permitindo a captura de expressões faciais de uma segunda pessoa e a sobreposição no rosto de um indivíduo no vídeo original (Solon, 2017).

Conteúdos Fabricados: Inclui a criação de informações falsas ou documentos fraudulentos para dar suporte a uma história fictícia. Conforme a perspectiva de Gomes, a categoria de "Conteúdo Fabricado" pode abranger as fakes news que circulam, oferecendo supostas curas para a Covid-19, sem base científica, tal como a sugestão de beber água quente, consumir Vitamina C ou chá de erva-doce (Gomes, 2020). [2]

1.3.2 Exemplos Históricos de Notícias Falsas

A mentira, a desinformação e os rumores difundidos socialmente não são um fenômeno recente, de modo que expressões prejudiciais semelhantes aos textos e *tweets* [3]maldosos vistos atualmente têm raízes que remontam uma ampla variedade de períodos históricos, incluindo os mais antigos, sendo, portanto, anteriores à era digital e as redes sociais, conforme argumenta Robert Darnton, historiador norte-americano, em seu artigo intitulado "*The True History of Fake news*" (2017), publicado pela Revista "*The New York Review of Books*".

O *International Center for Journalists* (ICFJ) publicou o guia "*A Short Guide to the History of Fake news and Disinformation*", no qual relata que o primeiro registro na história sobre a prática remonta a 44 a.c., quando Octaviano instaurou uma campanha difamatória em desfavor do Imperador Marco Antônio, através da utilização de curtos slogans amoedados para atingir a sua reputação. Tudo isso tinha a finalidade de obter vantagens na luta pelo controle do Império Romano. E isso realmente aconteceu, Octaviano se tornou o imperador romano Augusto (Marioni e Galassi, 2020; Icfj, 2018).

---

[2] Como exemplo, temos as fakes news que foram espalhadas no ano de 2021, durante a Pandemia da Covid-19, quando foram disseminadas fake news alegando que a ivermectina tinha uma eficácia de 90% na prevenção do vírus. No entanto, essa afirmação foi desmentida pela própria empresa fabricante do medicamento, que enfatizou a ausência de comprovação de eficácia contra a doença (Fato, 2021).

[3] "*Tweets* ou tuítes (em português) representam as mensagens que os usuários postam no Twitter, famoso microblog nos dias de hoje". Dicionário Informal. Diferença entre "*tweet*" e "Twitter". Disponível em: https://www.dicionarioinformal.com.br/diferenca-entre/tweet/twitter.

“Os Libelos de sangue” é outro exemplo histórico marcante de como a propagação de boatos pode prejudicar uma sociedade. Tratava-se de acusações que diziam respeito a sacrifícios humanos, principalmente de crianças, em rituais religiosos. Judeus frequentemente foram alvo, sendo isso uma expressão do antissemitismo medieval. O historiador Yuval Noah Harari, em sua obra “21 Lições para o Século 21” (2018), exemplifica essa prática com o caso de Hugh, um menino inglês encontrado morto num poço em 1255, na Inglaterra.

Conforme Harari (2018), Matthew Paris, um cronista inglês, escreveu uma versão literária na qual judeus da Inglaterra se reuniram numa cidade chamada Lincoln para torturar e crucificar o menino sequestrado. Mesmo sem evidências, essa história ganhou detalhes e popularidade ao longo do tempo, reforçando o antissemitismo e resultando em perseguição e massacres de comunidades judaicas na Idade Média. Isso contribuiu para a expulsão de toda a população judaica da Inglaterra em 1290. (Harari, 2018)

A invenção da prensa de Gutenberg em 1493 marcou o início da Revolução da Imprensa, que provocou mudanças essenciais na forma como as notícias falsas e os boatos eram disseminados à época. Segundo Robert Darnton (2017), o século XVIII viu o surgimento dos tabloides, incluindo o *The Morning Post,* fundado em 1772 por Henry Bate na Inglaterra, que se caracterizava por conter principalmente notícias falsas. Em 1874, o jornal publicou uma falsa notícia sobre a rainha Maria Antonieta da França, alegando que ela estava pagando por serviços sexuais:

> A rainha francesa tem carinho pelos britânicos. Na verdade, a maioria de seus favoritos vem daquele país, mas ela prefere é o Senhor W. Sabe-se que esse cavalheiro tinha a carteira vazia quando chegou a Paris, mas agora leva uma vida cheia de elegância, bom gosto e moda. Ele mantém suas carruagens, seus uniformes e mesa sem economizar e com todo o esplendor (Darnton, 2017, on-line).

Em 1835, o jornal New York Sun publicou uma série de seis artigos sobre a descoberta de vida na lua. Os relatos mencionaram criaturas fantásticas como unicórnios e humanóides. Embora a intenção fosse satírica, com o objetivo de zombaria, os leitores não perceberam, levando até cientistas da Universidade de Yale a serem enganados. O caso que ficou conhecido como “*The Great Moon Hoax* (A Farsa da Lua Cheia)”, foi desmentido pelo jornal naquele mesmo ano (Sun, 2010).

Num contexto mais notável, antes da era da internet e dos meios digitais, também existem exemplos emblemáticos de notícias fraudulentas sendo empregadas como instrumento de propaganda de guerra, como durante a Primeira e a Segunda Guerra Mundial, de acordo com o Jornal El País (2018). A historiadora francesa Annette Becker pesquisou o impacto dessa prática nesses dois conflitos mundiais, observando que as operações

psicológicas dos Aliados contra os alemães entre 1914 e 1918, através da disseminação de notícias falsas que os acusavam de brutalidades, tiveram repercussões negativas na compreensão das atrocidades nazistas durante o Holocausto entre 1939 e 1945.

Sob este escopo, a utilização de notícias falsas como propaganda visava ludibriar, criando realidades alternativas, influenciando opiniões públicas para alcançar metas econômicas e políticas específicas. A preocupação com a disseminação de equívocos e seus mecanismos não é recente, Marc Bloch (2012) abordou essa questão em seu ensaio "*Réflexions d'Un Historien Sur les Fausses Nouvelles de la Guerre*" (Reflexões de um historiador sobre notícias falsas de guerra), publicado originalmente em 1921. No ensaio, Bloch (2012) examinou o papel das notícias falsas durante a Primeira Guerra Mundial, abordando sua origem e propagação. O conteúdo se mantém relevante, ao ponto que poderia ser aplicado à era do *Brexit* e Donald Trump, redes sociais e mensagens virais.

> As notícias falsas mobilizaram as massas. As notícias falsas, em todas as suas formas, encheram a vida da humanidade. Como nascem? De que elementos extraem sua substância? Como se propagam e crescem? [...] Um erro só se propaga e se amplifica, só ganha vida com uma condição: encontrar um caldo de cultivo favorável na sociedade onde se expande. Nele, de forma inconsciente, os homens expressam seus preconceitos, seus ódios, seus temores, todas as suas emoções (Bloch, 2012, on-line).

Num cenário mais recente, com a revolução da internet e da ascensão das redes sociais, evidencia-se dois acontecimentos de conhecimento global, ocorridos no ano de 2016, que possuem interferência de diversas fake news. O primeiro diz respeito à saída do Reino Unido da União Europeia (UE), conhecido como Brexit. Essa decisão obteve auxílio de uma empresa de mineração e análise de dados, que utilizou um estudo sobre usuários de redes sociais para aplicar propaganda computacional e disseminar fake news em apoio ao *Brexit*, a campanha *Leave* (Bilney, 2016). A segunda se refere à candidatura do empresário republicano Donald Trump à presidência dos Estados Unidos da América. Segundo Marinoni e Galassi (2020), nessas eleições, o termo foi inicialmente usado para descrever sites e blogs que surgiram na cobertura da corrida presidencial, divulgando informações falsas com a aparência de jornalismo e adotado, posteriormente, pelo ex-presidente Trump.

O Brasil também desempenhou seu papel na disseminação de fake news, como evidenciado no caso do impeachment da ex-presidente Dilma Rousseff. O ex-presidente da Câmara dos Deputados, Eduardo Cunha, acolheu o pedido de impeachment apresentado por Hélio Bicudo, Miguel Reale Júnior e Janaína Paschoal, alegando que a presidente havia cometido crime de responsabilidade devido às "pedaladas fiscais". Em 31 de agosto de 2016,

o Senado concluiu o processo de impeachment de Dilma Rousseff, com 61 votos favoráveis e 20 contrários durante o julgamento (Notícias, 2016).

Segundo um estudo realizado pelo Grupo de Pesquisa em Políticas Públicas de Acesso à Informação da USP, citado pela BBC Brasil, três das cinco reportagens mais amplamente compartilhadas no Brasil no Facebook durante a semana do processo de impeachment eram falsas. O estudo avaliou o desempenho de 8.290 reportagens provenientes de 117 fontes, incluindo jornais, revistas, sites e blogs (Senra, 2016).

Ricardo Senra (2016) ainda evidencia que, entre as notícias categorizadas como conteúdos fabricados disseminadas durante a semana do impeachment, dois títulos se destacam: “Polícia Federal quer saber os motivos para Dilma doar R$30 bilhões a Friboi” e “Presidente do PDT ordena que militância pró-Dilma vá armada no domingo: ’Atirar para matar’”. Essas notícias foram veiculadas pelos portais Pensa Brasil e Diário do Brasil, respectivamente.

O artigo publicado no site Pensa Brasil (Zatti, 2016) ocupou a terceira posição no ranking geral da semana, obtendo 90.150 compartilhamentos nas redes sociais. Enquanto isso, a segunda notícia, que relata o suposto pedido do Presidente do PDT para que a militância pró-Dilma fosse armada no dia da votação do impeachment, alcançou o quarto lugar no ranking, com 65.737 compartilhamentos. Se considerarmos que a média de seguidores por usuário pode atingir 200, essas notícias têm o potencial de alcançar praticamente toda a população brasileira (Martins, 2017).

1.4 A *DEEPFAKE* E SUA RELAÇÃO COM AS FAKES NEWS

O avanço da tecnologia traz para a sociedade oportunidades que antes eram impensáveis e que têm o poder de mudar a maneira como as pessoas se relacionam. Ao abordar sobre a *deepfake* no artigo intitulado “*Deep fakes: A looming challenge for privacy, democracy, and national security*” (2018), Robert Chesney e Danielle Cintron destacam que estas são vídeos, sons ou imagens projetados para fazer com que uma pessoa pareça estar dizendo ou fazendo algo que nunca disse ou fez. Isso traz à tona uma série de questões complexas no âmbito político, tecnológico e jurídico. À medida que os métodos de criação, baseados em inteligência artificial, se tornam mais avançados e acessíveis, esses vídeos têm o potencial de criar novas formas de desinformação e assédio. Portanto, fica evidente que a disseminação desse conteúdo é mais prejudicial do que a própria tecnologia de inteligência artificial em si.

Os primeiros exemplos amplamente conhecidos de vídeos manipulados por inteligência artificial, nos quais rostos eram trocados de forma amadora, surgiram em novembro de 2017. Isso aconteceu quando um usuário da rede chamada *Reddit*, com o nome "*deepfakes*", compartilhou uma série de vídeos nos quais ele colocou os rostos de atrizes famosas, como Gal Gadot e Scarlett Johansson, em corpos de outros atores em conteúdo pornográfico. Embora o termo original fosse *fakevideo*, a partir desse momento, a mídia e o público em geral começaram a usar o termo "*deepfakes*" para se referir a esse tipo de vídeo, que utiliza técnicas de *deep learning* (aprendizado profundo) ou *machine learning* (aprendizado de máquina) para mesclar ou criar imagens de corpos e rostos humanos de maneira enganosa (Paris; Donovan, 2019, apud Santaella; Salgado, 2021).

A indústria cinematográfica também já se utilizou dessa técnica. Um exemplo disso ocorreu no filme "*Rogue One*: Uma História *Star Wars*" (2016), que faz parte da série homônima. Neste filme, alguns personagens foram recriados, como no caso mais intrigante do Comandante Tarkin, originalmente interpretado pelo britânico Peter Cushing, que havia falecido em 1994. Utilizando técnicas computacionais, foi possível realizar o que é conhecido como "reconstrução digital" da imagem do ator falecido. Isso levanta questões legais, como a necessidade de autorização dos herdeiros para a reconstrução da imagem. Vale ressaltar que essa situação é peculiar, pois não se trata simplesmente de reproduzir imagens já capturadas no passado, mas sim de criar novas imagens com base em capturas anteriores (Raphael, 2018).

Embora os primeiros casos de *deepfake* tenha se concentrado em figuras políticas, celebridades e artistas, fora previsto que nos próximos tempos essas tecnologias serão cada vez mais utilizadas para criar conteúdo sexual não consensual, praticar o *cyberbullying*, produzir provas de vídeo falsas em processos judiciais, promover a sabotagem política, disseminar propaganda terrorista, extorquir pessoas, influenciar o mercado financeiro e espalhar informações falsas, de acordo com as pesquisas de Hasan e Salah (2019) e Maras e Alexandrou (2019).

As *deepfakes* representam uma ferramenta poderosa para criar e disseminar notícias falsas. Nina Schick (2019) destaca que essa tecnologia é uma inovação digital que permite a criação de vídeos capazes de simular diversos tipos de conteúdo por meio de manipulações, incluindo a criação de discursos políticos fictícios, trazendo implicações substanciais na propagação de notícias falsas e na influência sobre a opinião pública, pois conecta erroneamente o nome e a identidade de uma pessoa a ideias e ações que, por natureza, não são verdadeiras nem refletem a realidade sobre esse indivíduo.

De acordo com Koopman, Macarulla Rodriguez e Geradts (2018), a crescente capacidade de criar resultados fotorrealistas por meio de *deepfakes* tem levado ao aumento da demanda por métodos de autenticação para detectar manipulações. Por conseguinte, as *deepfakes* se tornam um problema cada vez mais relevante na era das notícias falsas, afetando não apenas a esfera das notícias, mas também impactando jornalistas de vídeo, provedores de hospedagem de sites e usuários de mídia social.

Outrossim, com o aumento do número de imagens digitais, com a adoção de novas tecnologias, como câmeras, smartphones e tablets mais modernos, as mídias sociais como Facebook, Instagram e Twitter aumentam ainda mais a sua distribuição de fotografias e vídeos. Dessa forma, as ferramentas de manipulação de imagens digitalmente avançaram gradativamente, e os softwares e aplicativos para smartphones tornaram-se bastante simples para usuários que manuseiam imagens com facilidade (Bunk et. al, 2017).

Atualmente, já existem ferramentas de manipulação de vídeos acessíveis e de uso simplificado, até mesmo para indivíduos com pouca experiência em tecnologia, como o *DeepFaceLab*, que amplifica o risco associado às *deepfakes* na criação e disseminação de notícias falsas, revelando a facilidade com que podem ser usadas de forma prejudicial. Elas podem ser operadas por meio de softwares comuns e gratuitos, utilizando equipamentos simples, como um computador doméstico. Esse fenômeno de criação de *deepfakes* por pessoas sem conhecimento avançado em tecnologia é chamado por outros autores de "*cheap fakes*" (falsos baratos) (Karnouskos, 2020, apud Santaella; Salgado, 2021).

Como exemplo de facilidade na criação de conteúdo manipulado, surge uma aplicação para smartphones que tem a capacidade de criar automaticamente rostos em fotografias, produzindo imagens extremamente realistas, chamada *FaceApp*. Este aplicativo possibilita a alteração de características como rosto, cabelo, sexo, idade e diversos outros detalhes utilizando apenas o dispositivo móvel, conforme destacado por Korshunov e Marcel (2018) e Güera e Delp (2018).

Em um cenário diferente, mesmo que as *deepfakes* não tenham a capacidade de enganar os espectadores, elas podem instilar um profundo ceticismo nas pessoas em relação às notícias que consomem, tendo em vista que as *deepfakes* têm o potencial de abalar as percepções individuais de verdade e falsidade, gerando incertezas sobre a autenticidade do conteúdo divulgado por veículos de notícias, mais especificamente por meio das redes sociais. Dessa maneira, acaba gerando uma diminuição da confiança em relação ao que é compartilhado on-line.

> Se as *deepfakes*, juntamente com outros métodos de desinformação, conseguirem aumentar a incerteza, uma das principais implicações pode ser uma redução da confiança nas notícias nas redes sociais, onde os *deepfakes* provavelmente circularão com mais frequência. (Vaccari. 2020, on-line).

Com a disseminação das *deepfakes*, como destacado por Korshunov e Marcel (2018) e Güera e Delp (2018), as ferramentas para a criação de vídeos *deepfake* têm sido amplamente empregadas na produção de notícias falsas envolvendo celebridades. Algumas plataformas, como o Twitter, já proibiram a veiculação desse tipo de vídeo. No entanto, devido à sua qualidade quase realista, esses vídeos têm se tornado alvo para a geração de conteúdos ilícitos, falsos e prejudiciais, que são usados até mesmo para criar tensões políticas. Consequentemente, esses fenômenos estão atraindo a atenção de autoridades governamentais e agências reguladoras.

1.5 O FUNCIONAMENTO DA TECNOLOGIA *DEEPFAKE* E SUA APLICAÇÃO NA CRIAÇÃO DO CONTEÚDO MANIPULADO

Como dito anteriormente, a *deepfake* é o resultado de uma técnica baseada num tipo específico de *machine learning* (aprendizado de máquina), chamada "*deep learning*" (aprendizado profundo). Nessa técnica há um conjunto de algoritmos chamados "redes neurais" que aprendem a identificar regras e reproduzir padrões ao analisar grandes volumes de dados armazenados. Elas surgem de uma variante específica do aprendizado profundo, que envolve a utilização de pares de algoritmos em algo chamado "redes generativas adversariais" ou GANs. Em uma GAN, há dois algoritmos em jogo: o "gerador" e o "discriminador". O gerador cria conteúdo artificial com base em dados de origem (por exemplo, criando imagens de gatos falsas a partir de um conjunto de dados de imagens reais de gatos). Enquanto isso, o discriminador tenta identificar o conteúdo artificial, ou seja, distinguir as imagens de gatos falsas das reais. A chave para o funcionamento das GANs é que esses dois algoritmos estão em constante competição e aprendizado um com o outro, levando a melhorias rápidas e permitindo que as GANs gerem conteúdo de áudio e vídeo que é altamente realista, porém falso (Chesney, 2019).

No processo de criação de *deepfake* é necessário que se alimente o banco de dados da rede neural da inteligência artificial com uma quantidade significativa de imagens da pessoa que se deseja retratar e da pessoa cujo rosto será substituído. Os algoritmos de IA utilizam esse banco de dados para aprender como as imagens se comportam em diferentes ângulos e iluminação, continuando até que o programa seja capaz de identificar pontos comuns entre as duas faces e, de certa forma, "costurá-las" uma sobre a outra. Desse modo, eles se tornam

capazes de criar reproduções realistas de manipulação de mídia nas quais um rosto é sobreposto ao outro (Cabral, 2018).

1.5.1 *Deepfake* na criação de conteúdo falso

Atualmente, é possível categorizar as falsificações em quatro tipos principais, com base no grau de manipulação empregado, conforme apontado por Dang et al. (2019). Tolosana et al. (2016) fornece uma análise detalhada de cada um desses tipos, que serão brevemente descritos a seguir, em ordem crescente de intensidade na manipulação.

Expressões Faciais: Essa categoria envolve a alteração da expressão facial de uma pessoa. A modificação pode ocorrer de duas maneiras: a transferência da expressão de uma pessoa para outra, chamada de "*source-to-target*", e a autorrepresentação, na qual a mesma imagem atua como origem e destino da manipulação. Uma técnica amplamente conhecida para criar esse tipo de manipulação é chamada de *Face2Face* (Thies et al., 2016).

Atributos faciais: Esse processo envolve a alteração de características como cor da pele, cabelo, gênero, idade ou até mesmo a adição de acessórios, como óculos. Normalmente, são empregadas Redes Neurais Generativas Adversariais (GANs) para realizar esse tipo de manipulação (Choi et al., 2018). Um exemplo conhecido de aplicativo que funciona com base nesse tipo de manipulação é o popular *FaceApp* (FaceApp, 2017).

Troca de Identidades (Face Swap): Este é possivelmente o tipo de manipulação mais reconhecido, pois serviu como precursor para o atual cenário de pesquisa em *deepfakes* e é amplamente visível em vídeos do YouTube, como no canal do brasileiro Bruno Sartori, que usa essas manipulações para criar sátiras políticas e se autodenomina "*deepfaker*" (Sartori, 2012). Nesse tipo de manipulação há substituição do rosto de uma pessoa pelo rosto de outra. Existem duas abordagens principais para realizar esse tipo de manipulação: 1) a abordagem clássica, que se baseia em técnicas de computação gráfica, como a técnica *FaceSwap* (Kowalski, 2018), e 2) a abordagem mais recente, que utiliza técnicas de *deep learning*, conhecida como *Deepfakes*. Um exemplo comercial acessível ao público que emprega essa tecnologia é o aplicativo ZAO (Loubak, 2019).

Síntese facial: Essa forma de manipulação envolve a criação de rostos completamente novos, ou seja, a geração de faces que são inteiramente fictícias. A síntese facial costuma ser produzida com a ajuda de redes GAN (Redes Generativas Adversariais), conforme demonstrado por Karras, Laine e Alla (2019). Os resultados obtidos com essa abordagem surpreendem pela sua alta qualidade e realismo, conforme destacado por West e Bergstrom (2019) e também por Wang (2019).

Neste cenário, é evidente que as *deepfakes* assumem um papel de destaque como um dos principais métodos de manipulação de mídia empregados para disseminar notícias falsas na atualidade. Sua capacidade de criar conteúdo audiovisual altamente convincente e enganador tem desafiado a confiabilidade da informação na era tecnológica, levando a uma crescente conscientização sobre os perigos das *deepfakes* em diversas esferas, desde a política até a mídia de entretenimento. Portanto, torna-se imperativo assegurar a proteção jurídica do direito à informação constitucionalmente estabelecida, considerando, principalmente, as mudanças trazidas na era digital.

2 A ERA DIGITAL E A TUTELA JURÍDICA DO DIREITO À INFORMAÇÃO

O capítulo anterior explora a ascensão das *deepfakes* e seu impacto na disseminação de notícias falsas na era digital. Agora, ao adentrar no segundo capítulo, mergulhar-se-á na relação entre a era digital e a tutela jurídica do direito à informação. Neste universo de avanços tecnológicos acelerados e mudanças sísmicas na maneira como se consome e compartilha informações, examina-se como os sistemas legais se adaptam para garantir a integridade da informação e preservar os pilares fundamentais da sociedade democrática.

2.1 A CONSTITUIÇÃO FEDERAL DE 1988 E O DIREITO À LIBERDADE DE EXPRESSÃO, PRIVACIDADE E INFORMAÇÃO

A Constituição Federal de 1988, chamada de "Constituição Cidadã" e promulgada em cinco de outubro do mesmo ano, é o mais relevante instrumento de garantia do Estado Democrático de Direito. A CRFB/1988 surge do ideal de um "dever-ser" e constitui um conjunto de normas jurídicas fundamentais, estabelecendo, inclusive, os direitos e deveres dos cidadãos. Ela representa a Lei Maior, e todas as demais normas do ordenamento jurídico brasileiro devem estar em conformidade com ela, estando subordinadas a essa premissa.

Ao discorrer sobre a Carta Magna, Rodrigo Padilha (2014) destaca que a atual Constituição representa, primordialmente, uma promissora visão para um futuro mais esperançoso. Ela engloba direitos nunca antes abordados em documentos constitucionais anteriores, posicionando-se como a mais abrangente na história no que diz respeito aos direitos individuais, coletivos e sociais. Além disso, é a Constituição que mais estabeleceu medidas para salvaguardar esses direitos, enquanto expandiu significativamente o escopo de controle de constitucionalidade das leis, visando assegurar uma maior solidez ao sistema normativo.

A evolução constitucional possibilitou o surgimento de direitos, como informação, liberdade de expressão, privacidade e proteção de dados, os quais estão claramente expressos no artigo 5º da Constituição Federal. Esses direitos constituem uma parcela dos direitos fundamentais consagrados na Constituição, sendo garantias protetivas que garantem ao ser humano o mínimo existencial para uma vida digna em sociedade. O artigo 1° da Lei n.º 5.250, de 9 de fevereiro de 1967, que regulamenta o direito à liberdade de manifestação do pensamento e de informação, dispõe que:

> Art. 1º É livre a manifestação do pensamento e a procura, o recebimento e a difusão de informações ou idéias, por qualquer meio, e sem dependência de censura, respondendo cada um, nos termos da lei, pelos abusos que cometer (Brasil, 1967).

Seguindo esta mesma linha de raciocínio, a Constituição Federal de 1988 contempla em seu texto o direito à liberdade de expressão, de informação e de manifestação do pensamento, conforme preconiza o seu art. 220: "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição". O § 2º do supramencionado artigo disciplina que "é vedada toda e qualquer censura de natureza política, ideológica e artística" (Brasil, 1988).

Atualmente, a liberdade de expressão engloba o direito de liberdade de informação e o direito de liberdade de imprensa, que constitui o direito de informar e ser informado, como anteriormente acentuado. A livre expressão deve ser exercida em sua plenitude, baseando-se na construção do justo e do igual na sociedade, assim como no princípio do mínimo existencial, intrínseco ao homem.

O direito de liberdade de informação constitui um elemento essencial para a garantia do direito à privacidade, "não porque ela permita a formação de uma opinião pública esclarecida, capaz de respeitar e se posicionar ao lado de um indivíduo que, frente às admoestações da turba e da burocracia estatal, advoga um interesse legítimo", mas porque a transparência é crucial para promover a clareza nos negócios públicos, assim como garantir transparência nas decisões sociais que podem afetar os direitos fundamentais das pessoas (Miranda, 1996. p. 145 e 146).

Acerca dessa lógica, o art. 5º, X, da Constituição da República estabelece, de forma expressa, a inviolabilidade a intimidade, a vida íntima e a honra indivíduos, sendo-lhe garantido o direito de ser indenizado por prejuízo material, moral ou à sua imagem, caso alguém venha a se sentir lesado.

Destarte, é comum que a liberdade de expressão esbarra com outros direitos e garantias individuais, como o direito à privacidade. Esse direito constitui a prerrogativa de escolha pessoal do indivíduo sobre a possibilidade de opor-se a invasão de terceiros em sua vida privada, bem como na vida familiar, podendo inclusive, impedir que tais pessoas tenham acesso e a divulgação de informações acerca da privacidade de cada um, compreendendo o mínimo existencial humano conforme acentua (Bastos; Martins, 2004).

Assim, o direito à privacidade representa a faculdade de excluir ou não o conhecimento de informações pessoais a partir de terceiros. Principalmente, no que concerne ao modo de ser e viver de alguém. Ou seja, esse direito constitui a garantia de impossibilitar a ingerência alheia na vida íntima. Segundo Elimar Szaniawski, o direito à privacidade é:

> O direito subjetivo que consiste no poder de toda pessoa assegurar a proteção dos interesses extrapatrimoniais, de impedir a intrusão, a divulgação e a investigação, na sua vida privada, garantindo a paz, a liberdade da vida pessoal e familiar, criando o dever jurídico em relação a terceiros de não se imiscuírem na vida privada alheia (2005, p. 153).

Embora haja garantia plena do direito à liberdade, esse direito também não é absoluto, principalmente quando na realização de alguma atividade que possa causar dano a outrem. Na atualidade, por meio da internet, a liberdade de expressão se depara com um espaço amplo para o seu exercício, o que se torna propício para a disseminação de conteúdo e informações que comprometem o debate e fomenta a circulação de notícias falsas e desinformação(Oliveira e Gomes, 2019). [4]

Sérgio Branco (2018) acentua que o limite para a liberdade de expressão está na verdade. O que não significa um obstáculo para a execução do jornalismo ou veiculação de notícia, mas um dever de precaução para aqueles que emitem algum tipo de informação. De igual modo, toda e qualquer notícia deve ser apurada com a finalidade de verificação da confiabilidade e veracidade, considerando, primordialmente, que estão aptas a formar opiniões.

Desse modo, os limites quanto ao exercício da liberdade devem existir e são válidos, contudo, não deve ser associado à sua negação, ao contrário, seus limites permitem que o homem escolha entre as várias possibilidades existentes e assume suas respectivas consequências (Paesani, 2013).

Por sua vez, o direito à informação, conforme destacado por Marco Cepik (2000, p. 4), representa uma gama de princípios legais que objetivam "assegurar que qualquer pessoa ou organização tenha acesso a dados sobre si mesma que tenham sido coletados e estejam armazenados em arquivos e bancos de dados governamentais e privados", bem como informações públicas que digam respeito ao governo, a administração pública e o país, ressalvados "o direito à privacidade, o sigilo comercial e os segredos governamentais previstos em lei".

Esse direito emerge da conscientização democrática e do progresso das sociedades. A conquista de novos direitos ocorre de maneira gradual, muitas vezes em resposta aos avanços tecnológicos (Bobbio, 2004, p. 13).

Edilson Farias (2004) assegura que o acesso à informação possui uma grande importância para o "pleno exercício dos direitos sociais e individuais e para o bem-estar de

[4] Corroborando com esse entendimento, a Comissão dos Direitos Humanos da Ordem dos Advogados de Portugal (2006, p.71) preceitua que "a liberdade de expressão é um direito fundamental, mas não um direito absoluto (...) Há limites, há fronteiras, mas são perigosas e difíceis de traçar. Diremos apenas que os limites são inultrapassáveis".

uma sociedade fraterna", ideologia reconhecida no preâmbulo da Constituição Federal de 1988. De mais a mais, o recebimento de informações está diretamente relacionado ao exercício digno da cidadania e da soberania popular. De modo que, esses pilares estariam comprometidos se esse direito fundamental fosse negligenciado.

José Afonso da Silva (2005, p. 245 e 246), substanciado nas contribuições de Albino Greco, ao discorrer sobre o direito à informação e a liberdade de informação como componentes essenciais para a plena efetivação da cidadania, expõe que:

> Como esclarece Albino Greco, por 'informação' se entende 'o conhecimento de fatos, de acontecimentos, de situações de interesse geral e particular que implica, do ponto de vista jurídico, duas direções: a do direito de informar e a do direito de ser informado'. O mesmo é dizer que a liberdade de informação compreende a liberdade de informar e a liberdade de ser informado. A primeira, observa Albino Greco, coincide com a liberdade de manifestação do pensamento pela palavra, por escrito ou por qualquer outro meio de difusão; a segunda indica o interesse sempre crescente da coletividade para que tanto os indivíduos como a comunidade estejam informados para o exercício consciente das liberdades públicas. Nesse sentido, a liberdade de informação compreende a procura, o acesso, o recebimento e a difusão de informações ou idéias, por qualquer meio, e sem dependência de censura, respondendo cada qual pelos abusos que cometer[...] (Silva, p. 245 e 246, 2005).

Nesse contexto, depreende-se que o direito à informação engloba a liberdade de receber, buscar e compartilhar informações, sem que haja algum tipo de censura. Em síntese, o direito à informação abrange a faculdade de comunicar e divulgar informações sem a presença de obstáculos, sendo, enquanto direito de liberdade, o acesso aos meios para se informar (Canotilho e Moreira, 2014).

Além disso, o direito à informação, amplo e sem restrição, também abrange a liberdade de selecionar informações e a sua pluralidade de fontes, garantindo que as pessoas não sejam impedidas de acessar as informações que desejam. Essa prerrogativa deve ser proporcionada por todos os meios de comunicação, bem como, pelo poder público, cumprindo seu dever de publicidade (Lindemberg, 2007).

Outrossim, a avaliação da veracidade da informação deve levar em conta não apenas o discurso, mas também a rede de convenções sociais, tradições e a cultura daqueles que consomem essa informação. Enquanto o direito à informação é garantido constitucionalmente como um meio de viabilizar o Estado Democrático de Direito, ele não deve ser confundido com a liberdade de pensamento e tampouco com o direito de expressar opiniões sobre um determinado tema. A liberdade de pensamento representa uma das facetas da liberdade num sentido amplo, que inclui as liberdades de opinião, informação e acesso ao conhecimento (Sundfeld, 1995).

Com o advento da Constituição Federal de 1988, o Brasil experimentou um fortalecimento da prerrogativa da liberdade de informação, que favoreceu a propagação de notícias não-verídicas ou sem fundamento fundamentado na construção de verdade própria. Desse modo, é imperativo observar que o legislador constituinte demonstrou uma maior preocupação com a censura prévia, deixando de legislar sobre a disseminação de informações falsas. Na era da democracia digital, o direito à informação precisa enfrentar desafios consideráveis devido à existência de grupos e bolhas ideológicas. A personalização extrema do conteúdo on-line, facilitada por algoritmos e robôs, leva a uma situação paradoxal em que o direito à informação verdadeira é afetado. As plataformas de conteúdo e redes sociais têm a tendência de oferecer aos usuários aquilo que eles já gostam e concordam, criando um ciclo de reforço das próprias opiniões e visões de mundo (Assis, 2020).

Na perspectiva de Luana Assis (2020), a produção de notícias falsas é uma atividade lucrativa para os seus criadores, isso porque cada clique e compartilhamento desse tipo de conteúdo é revertido em receita de capital para aquele ou aqueles que lhe deram origem. Além disso, geram também capital político com o poder de levar candidatos à presidência e lá mantê-los.

Neste contexto, o acesso e a liberdade de informação não podem constituir um direito absoluto, sendo passível de restrição à medida que transgrida outros valores constitucionalmente importantes. Ou seja, o acesso à informação deverá ser controlado com o objetivo de evitar a violação da privacidade, assim como outros direitos intrínsecos ao ser humano (Siqueira e Ferrari, 2016).

É fundamental reconhecer que nenhum direito é absoluto. Além disso, a liberdade de expressão está intrinsecamente ligada à informação precisa e honesta. Para formar opiniões livres, é necessário ter conhecimento da realidade. Por isso, a mentira é preocupante, pois obstrui a informação ao ocultar ou distorcer a verdade factual.

2.2 A LEI N. 12.965/2014 E A REGULAMENTAÇÃO DA INTERNET NO BRASIL

A expansão do espaço cibernético, fomentado pela internet e outros avanços tecnológicos, trouxe como consequência um novo mundo sem regulamentação e normas jurídicas aplicáveis e, portanto, sem responsabilização para as transgressões on-line. Isso gerou, em 2009, diversas discussões acerca da necessidade de regulamentar e normatizar o universo digital, que originou um projeto de lei, cujo objetivo tratava-se da consolidação de

direitos e responsabilidades aplicáveis aos usuários da internet, especialmente, no âmbito cível (Prata, 2017).

Com a intensificação da discussão sobre a possibilidade de regulamentação da rede, entre os anos de 2009 a 2014, o Centro de Pesquisa e Sociedade (FGV) passou a analisar e debater a proposta de lei em concurso com a Secretaria de Assuntos Legislativos do Ministério da Justiça, que culminou no lançamento do que ficou amplamente conhecido como o Marco Civil da Internet. Também participaram desse processo os membros da sociedade civil e representantes de áreas técnicas e acadêmicas, através de plataforma on-line (Leite; Lemos, 2014). Os autores Willis Santiago Guerra Filho e Henrique Garbellini Carnio (2014, p.14), acentuam que:

> O caso das relações virtuais na rede mundial de computadores – cada dia mais avançadas, complexas e determinantes da vida – é uma dessas questões e a chamada Lei do Marco Civil da Internet parece se apresentar como um novo modelo que propicia o âmbito de novas respostas, pois as ovas perguntas e há algum tempo já estão postas e tem sido enfrentadas apenas com antigas respostas.

Diante do universo virtual que fornece ao indivíduo novas formas de relações interpessoais inimagináveis, o Marco Civil da Internet foi elaborado com a finalidade de legislar sobre um tema que, à priori, não possuía resposta para todos os aspectos apresentados.

Esse dispositivo normativo instituiu no ordenamento jurídico brasileiro a tutela de direitos e deveres no âmbito cibernético, mais especificamente no que diz respeito a utilização da internet, seja obtendo acesso por meio de computadores, seja por meio de tablets, celulares, smartphones ou quaisquer outros meios possíveis. A legislação em comento encontra-se dividida em 5 capítulos: (Capítulo I – Disposições Preliminares; Capítulo II – Dos direitos e garantias dos usuários; Capítulo III – Da provisão de conexão e de aplicações de internet; Capítulo IV – Da atuação do poder público e; Capítulo V – Disposições Finais).

A Lei n.º 12.965/2014, Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Essa lei é construída sob três pilares de sustentação: liberdade de expressão, privacidade e neutralidade de rede.

2.2.1 Da Liberdade de Expressão no Marco Civil da Internet

Como dito anteriormente, a livre expressão do pensamento constitui um direito fundamental, assegurado pela nossa Carta Magna nos artigos 5º, IV e 220, assim como o direito de resposta, crença e acesso à informação.

Na sociedade de informação, com um fluxo contínuo de circulação de conteúdo, principalmente nas mídias digitais, a liberdade de expressão torna-se um instrumento para

para manutenção do Estado Democrático de Direito, contudo, é necessário um controle da qualidade da informação compartilhada em rede. Ao discorrer sobre a liberdade, o filósofo francês Montesquieu (2003, p. 164) dispõe que:

> Em um Estado, isto é, em uma sociedade onde existem leis, a liberdade não pode consistir senão em poder fazer o que se deve querer, e em não ser constrangido a fazer o que não se deve desejar. [...] Deve-se sempre ter em vista o que é independência e o que é liberdade. Esta última é o direito de fazer tudo aquilo que as leis facultam; se um cidadão pudesse fazer tudo o que elas proíbem, não teria mais liberdade, uma vez que os outros teriam também este poder.

Na perspectiva do Marco Civil, a liberdade de expressão ou opinião se transforma num fundamento para a utilização da internet no Brasil, conforme preceitua o caput do seu art. 2º "a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão [...]". Além disso, tem como finalidade erradicar qualquer forma de censura na rede.

Entretanto, o exercício da liberdade de expressão deve ser feito de uma maneira que não viole o direito de terceiros. Assim, tendo em vista a imensidão do mundo digital, o usuário tem o dever de fazer uso consciente e responsável, nos limites da boa-fé. Corroborando com esse entendimento, a Declaração dos Direitos do Homem e do Cidadão (2017), em seu artigo 4º, disciplina que:

> No entanto, no que tangia aos particulares, o ideal era de se ter a mais ampla liberdade. Essa ideia está permeada na Art. 4º. A liberdade consiste em poder fazer tudo que não prejudique o próximo. Assim, o exercício dos direitos naturais de cada homem não tem por limites senão aqueles que asseguram aos outros membros da sociedade o gozo dos mesmos direitos. Estes limites apenas podem ser determinados pela lei.

A internet se apresenta como uma terra livre e, com uma gama de possibilidades de manifestação de opiniões e convicções por partes dos indivíduos, indiscriminadamente. Desse modo, a garantia do direito à liberdade de expressão do pensamento prevista pelo Marco Civil da Internet vem para assegurar a livre manifestação do pensamento do usuário, devendo, dentro dos limites da boa-fé e harmonia social, respeitar os direitos do outro, como o direito à imagem, à honra, à dignidade ou a qualquer outro direito, para que estes não venham a ser violados.

Ao tratar sobre a liberdade de expressão como um fundamento do Marco Civil da Internet, Damásio de Jesus e Milagre (2016) acentuam que a liberdade de opinião deve ser preservada, contanto que essa expressão não infrinja os direitos de terceiros. Assim, a lei em comento não permite que alguém consiga retirar informações da internet apenas porque se sente desconfortável ou desagrada com o que está sendo dito. Antes do Marco Civil, em

resposta a denúncias on-line, muitos provedores optavam por remover conteúdos, extrajudicialmente, por insegurança em mantê-los disponíveis.

Partindo desse pressuposto, pode-se concluir que o direito à liberdade de opinião, previsto pela Constituição Federal de 1998 e pela Lei n.º 12.965/14, visa permitir que todos usuários de rede, amplamente, possam desfrutá-lo. Ou seja, permite o gozo, nos mais diferentes meios que as redes de computadores oferecem, de manifestar-se acerca de qualquer tema ou matéria, desde que de forma responsável, haja vista que ao violar direitos de terceiros ou, até mesmo, exercê-lo anonimamente, poderá responder pelo dano causado, nos termos da legislação vigente.

2.2.2 Da Privacidade no Marco Civil da Internet

Utilizando-se do seu direito de livre expressão do pensamento e opinião, muitos usuários colocam na internet um grande número de informações e dados pessoais, como por exemplo, fotos íntimas suas e de outras pessoas, esta última muita das vezes sem autorização e conhecimento, acarretando na exposição indevida da imagem de terceiros.

Nessa seara, o direito à privacidade no âmbito virtual é colocado em questionamento, gerando diversos danos aos usuários das redes, bem como, não usuários, que tiveram suas informações ou qualquer outro elemento íntimo explorado na internet. Ao tentar conceituar tal direito, Marcelo Novelino (2012) argumenta que ele surge intrinsecamente da dignidade da pessoa humana, garantindo ao indivíduo o poder de controlar sua própria vida, sem supervisão de terceiros.

A proteção do direito à privacidade previsto na Constituição Federal de 1988, encontra-se, também, fundamenta na Lei do Lei do Marco Civil da Internet e constitui "primeira lei infraconstitucional que regulamenta o tema e bem esclarece ser cabível indenização por dano moral ou material decorrente de violações à intimidade e vida privada no âmbito da internet" (Jesus, 2014. p. 33).

A respeito da proteção do direito à privacidade conforme estabelecido na Lei do Marco Civil da Internet, Patricia Peck Pinheiro (2013) enfatiza que a vida privada dos usuários da internet constitui uma garantia e deve ser resguardada pela Lei 12. 965/2014, uma vez que as informações e dados pessoais dos internautas possuem, no cenário atual, valor monetário agregado e são, comumente, usadas para pagamento de serviços tidos como gratuitos. Essas informações fornecidas, muita das vezes, são armazenadas por muito tempo ou para sempre pelos provedores de internet, podendo ser utilizadas para qualquer finalidade.

Nesse contexto, o Marco Civil da Internet tem o propósito de assegurar a privacidade de informações e dados dos usuários, visando alcançar um padrão equivalente ao adotado por outros países. Esse objetivo complementa não apenas o texto Constitucional, mas também o Código de Defesa do Consumidor e o Código Civil, fortalecendo assim a garantia da guarda segura das informações dos consumidores. Ao abordar os dados tanto de usuários quanto de não usuários, a Lei 12.965/14 foi inequívoca ao especificar em seu artigo 10 que:

> Art. 10 – A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (Brasil, 2014).

Portanto, é imperativo consignar que, além da proteção de dados dos usuários, é devido, de mesmo modo, a proteção de dados de não-usuários da rede digital. Um exemplo disso seria o compartilhamento de fotos ou vídeos de um indivíduo que não divulgou esses dados na internet, mas que estavam originalmente em dispositivos, como celular, e foram posteriormente postados na rede mundial de computadores.

Na atualidade, é comum pessoas tirarem fotos e fazerem vídeos íntimos com o intuito de compartilhá-las com terceiros de suposta confiança ou armazenarem seus dados em algum dispositivo eletrônico. Nessas hipóteses, os dados devem ser preservados, tendo em vista que o seu compartilhamento na internet enseja violação substancial do direito à intimidade e privacidade, com a possibilidade de causa dos irreversíveis à imagem de uma pessoa.

Um caso notório que exemplifica o texto acima, aconteceu com a atriz brasileira Carolina Dieckmann quando houve o vazamento de suas fotos íntimas. Após a contração de serviços de informática, a atriz teve seus dados vazados, sem autorização e, tampouco consentimento, por aqueles que executaram o serviço. Tal atitude configura uma violação séria à honra e à imagem da atriz, levando-a a buscar reparação por meio do Poder Judiciário (G1, 2012).[5]

Ao garantir a proteção do direito à privacidade, o Marco Civil da Internet põe a salvo a proteção da privacidade como um todo, isso engloba qualquer informação textual ou audiovisual considerada privada. No que concerne ao conteúdo a ser protegido, a legislação supra enfatiza os dados pessoais, informações que podem identificar uma pessoa e que normalmente são utilizadas ou requeridas pelos provedores de acesso à internet ou provedores

[5] Esse acontecimento resultou na promulgação da Lei 12.737/12, que trata da tipificação dos crimes cibernéticos (Brasil, 2012).

de serviços no Brasil. Assim, com o Marco Civil, empresas ou prestadores poderão ser responsabilizados civilmente por transgressão ao que preconiza a lei (Jesus; Milagre, 2016).

2.2.3 Da Neutralidade de Rede no Marco Civil da Internet

O Princípio da Neutralidade da Rede não está presente no texto da Constituição Federal. O referido princípio fora incluído na nossa legislação, e por ela garantido, através do inciso IV do artigo 3º da Lei n.º 12.965/2014, no qual preconiza que: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] IV – preservação e garantia da neutralidade de rede". Em decorrência do referido dispositivo normativo que a garante, o legislador infraconstitucional dedicou a Seção I do Capítulo III do Marco Civil da Internet à neutralidade de rede, ao mesmo tempo em que concebe, objetivamente, o conceito do princípio da pesquisa, no artigo 9º da referida lei.

A par disso, o art. 9º da Lei n.º 12.965/2014, dispõe que: "Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".

Nas palavras de Vladimir Aras (2014, on-line): "a neutralidade é um corolário da isonomia, do princípio segundo o qual todos são iguais perante a lei, e que não pode haver discriminação do conteúdo que trafega na Internet". Nesse passo, é legítimo assegurar que a neutralidade de rede garante que não haja discriminação ou distinção em relação ao conteúdo que é enviado ou recebido no mundo cibernético. Isso significa a garantia da liberdade de expressão, assim como, impede o controle de informações por empresas ou entidades (Cardoso, 2023).

Como forma de melhor ilustrar a neutralidade de rede na prática, imagine a seguinte situação: determinada operadora que fornece internet e TV a cabo, por vontade própria, decide restringir o acesso à algum serviço de streaming, como Netflix ou Globoplay, diminuindo a qualidade da conexão enquanto o usuário acessa o serviço, o que levaria o usuário a ter uma experiência desagradável ao tentar assistir a um filme ou série on-line. A neutralidade da rede existe justamente para evitar que isso aconteça, garantindo que nenhum conteúdo possa ser privado ou reduzido em termos de qualidade por qualquer empresa (Cardoso, 2023).

Indubitavelmente, o uso da rede e a navegação na internet pela sociedade seria bastante limitado se não existisse a neutralidade de rede, uma vez que a sua utilização se daria de forma fracionada, levando em consideração o potencial econômico de cada usuário. Em

outras palavras, aquele que tivesse um maior poder econômico poderia obter um pacote de acesso à internet com uma qualidade maior do que aquelas pessoas com um poder econômico menor.

À luz do Princípio da Neutralidade, Damásio de Jesus e José Antonio Milagre (2016) defendem que todos os pacotes de dados precisam oferecer o mesmo tratamento de velocidade de tráfego, sendo vedado, ao provedor, a redução da velocidade de navegação considerando o conteúdo acessado, a origem e o destino, o serviço ou à aplicação utilizada e, ainda, o "terminal que acessa" determinado serviço. Os provedores são proibidos de privilegiar ou mitigar o tráfego de acordo com o que é acessado (*traffic shaping*).

Apesar de ser considerada um princípio, a neutralidade da rede possui algumas exceções de acordo com o Marco Civil da Internet. O artigo 9º da lei possibilita a restrição ou diminuição da qualidade nas hipóteses em que requisitos técnicos sejam imprescindíveis à prestação adequada dos serviços e aplicação, assim como a priorização de serviços emergenciais. Assim, entende-se que, nos momentos de congestionamento elevado no tráfego, poderá haver a redução da qualidade para que o serviço seja mantido, isso se necessário (Cardoso, 2023).

2.2.4 Lei n.º 13.709/2018 (Lei Geral De Proteção De Dados)

Em que pese a impossibilidade de solução do problema de *deepfake* que venha a surgir, enquanto não advém uma lei específica para regular esse tema, poderia se utilizar a recente Lei Geral de Proteção dos Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que começou a viger a partir deste ano.

Um dos principais problemas a ser enfrentado pelo LGPD se converge para a constante violação da privacidade e intimidade do outro, em razão do uso indevido de dados pessoais alheios por diferentes espectros sociais, o que inclui até mesmo corporações e órgãos governamentais. Nesse sentido, analisa Santos e Araújo (2017, p. 171):

> O ambiente da internet trouxe inúmeros desafios como a preservação da liberdade de expressão, a proteção da personalidade, a dificuldade de armazenamento de dados privados disponíveis na web, como fotos, textos, vídeos, a regulação das relações comerciais, a proteção dos direitos autorais, o anonimato para causar danos ou prejuízos a outros, as inúmeras fraudes para obtenção de vantagem, os danos causados pelos vírus, furto de dados mediante fraude.

Em seus arts. 2º e 7º, traz, além de outros, a proteção ao direito à imagem e à honra, com a implementação de uma série de medidas que impedem o uso de dados pessoais sem o consentimento do titular, visando a preservação da intimidade. Assim, mesmo que essa lei não trate especificamente dos usos com finalidades ilícitas de ferramentas como a Inteligência

Artificial (I.A.) para criação de *deepfake*, ela poderá ser utilizada, por enquanto, para suprir a lacuna existente no direito brasileiro.

No contexto das redes sociais, a mesma se aplica tanto às empresas que coletam dados dos usuários quanto aos usuários que compartilham seus próprios dados nas redes sociais. É importante que os usuários estejam cientes das informações que estão compartilhando e com quem estão compartilhando (Brasil, 2018).

As redes sociais são um dos principais alvos da Lei em questão, já que muitas delas coletam e processam dados pessoais de seus usuários de forma massiva e sem transparência. É exigido que as empresas de redes sociais obtenham o consentimento explícito de seus usuários para coletar e processar seus dados pessoais, além de fornecer informações claras sobre como esses dados serão usados (Brasil, 2021).

Já as empresas e organizações que coletam dados pessoais nas redes sociais devem adotar medidas de segurança apropriadas para proteger esses dados contra acessos não autorizados, perda ou roubo. Em caso de incidentes de segurança que afetem dados pessoais, as empresas devem notificar imediatamente os usuários afetados e a Autoridade Nacional de Proteção de Dados (Brasil, 2021).

Além disso, quanto à proteção aos direitos de personalidade, combina-se a sua utilização com o art. 5°, X da Constituição Federal, que trata o assunto de forma genérica, e com o Código Civil, que trata mais especificamente o tema, em seus arts. 11 ao 21, já que os direitos de personalidade, em específico o direito à imagem, foram violados com a prática do *deepfake*. Além do direito à honra, cabível também se desse episódio resultasse um abalo indenizável a esse outro direito de personalidade.

2.3 DESAFIOS E DEBATES EM TORNO DA RESPONSABILIZAÇÃO DAS PLATAFORMAS ON-LINE

O Instituto da Responsabilidade Civil, previsto no artigo 186 da Lei n.º 10.406/2002, mais conhecida como Código Civil Brasileiro, está ligado à compreensão de que não se deve causar danos ou prejuízos a outrem. Assim, a sua finalidade consiste em desencorajar práticas de condutas lesivas que comprometam os interesses de terceiros, de modo que, todo indivíduo que incorrer ato que viole ou danifique o outro comete ato ilícito e fica obrigado a reparar: “A definição de responsabilidade civil em seu sentido clássico consiste na obrigação de reparar danos que infringimos por nossa culpa e em certos casos determinados pela lei” (Farias; Rosenvald; Netto, 2020, p. 34).

Com base nisso, a designação “responsabilidade civil” alinha-se adequadamente com a ideia de violação ou não cumprimento de um dever jurídico, resultando em danos a terceiros e, por conseguinte, estabelecendo uma obrigação jurídica subsequente de reparar o dano causado. Em termos simples, implica na obrigação de compensar os danos causados pelo agente, resultando no dever de efetuar um pagamento pecuniário à vítima.

Conforme anteriormente destacado, a Constituição Federal de 1988, em seu artigo 5º, alvitra que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, garantido o direito à compensação por danos materiais ou morais resultantes de sua violação. (Brasil, 1988).

Diante disso, pode-se extrair que não violar tais prerrogativas representa um dever jurídico originário, ao passo que, sua violação constitui um dever jurídico sucessivo de reparação ao dano causado por sua ação ou omissão. Sobre o descumprimento do um dever jurídico originário, Sergio Cavalieri Filho pontua que:

> A violação de um dever jurídico configura o ilícito, que, quase sempre, acarreta dano para outrem, gerando um novo dever jurídico, qual seja, o de reparar o dano. Há, assim, um dever jurídico originário, chamado por alguns de primário, cuja violação gera um dever jurídico sucessivo, também chamado de secundário, que é o de indenizar o prejuízo. A título de exemplo, lembramos que todos têm o dever de respeitar a integridade física do ser humano. Tem-se, aí, um dever jurídico originário, correspondente a um direito absoluto. Para aquele que descumprir esse dever surgirá um outro dever jurídico: o da reparação do dano (Cavalieri, 2002, p. 2).

Portanto, é imperativo acentuar que a responsabilidade civil representa um dever jurídico subsequente, com o propósito de reparar o dano causado pela violação de um dever jurídico originário.

Diante disso, é imperativo consignar que a responsabilidade civil pode ser objetiva ou subjetiva. Essa primeira ocorre quando se identifica a existência de conexão entre o dano e quem o praticou (dano + nexo causal). Assim, o agente será responsabilizado independente da comprovação de culpa, conforme estabelecido no artigo 927, parágrafo único, do Código Civil de 2002: “Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem” (Brasil, 2002).

No que concerne à responsabilidade subjetiva, ela “se caracteriza por ser necessária a demonstração de culpa” (Fernandez, 2013, p. 167), ou seja, além da ação danosa e do nexo de causalidade, é necessário a comprovação de culpa de quem causou o prejuízo para que se possa falar em responsabilização.

No âmbito da Lei n.º 12.965/2014 observa-se a existência de dois tipos de provedores de internet: I) Provedores de Conexão (Operadoras Claro, Vivo, Tim) e; II) Provedores de Aplicações (Twitter, Tiktok, Instagram e Whatsapp). Assim é a perspectiva fornecida pelos professores Souza e Lemos (2016, p. 16):

> O Marco Civil faz uma distinção entre provedores de conexão (os que dão acesso à rede) e os de aplicações (como pesquisa, hospedagem, redes sociais e etc). Os primeiros não respondem pelos atos de seus usuários (art. 18) e os segundos apenas se não cumprirem ordem judicial (com exceção dos direitos autorais e de materiais de "pornografia de vingança", conforme os artigos 19 e seguintes).

Dito isso, fica compreendido que o provedor de conexão não será responsável pelo conteúdo disponibilizado por terceiros, enquanto, via de regra, o provedor de aplicações de internet poderá ser responsabilizado civilmente de forma subjetiva, de acordo com o artigo 19 da lei em comento.

Nesse contexto, o provedor de aplicações de internet só poderá ser responsabilizado por ações ilícitas de terceiros em sua plataforma caso descumpra uma decisão judicial. Em outras palavras, se por acaso determinado usuário publicar um conteúdo ofensivo à outrem e, o provedor de aplicação de internet recebe uma ordem judicial para remover esse conteúdo ilegal postado em sua plataforma e não cumpre essa ordem dentro do prazo estabelecido, ele poderá ser responsabilizado pelos danos decorrentes desse ato ilícito.

Por outro lado, é possível aplicar ao provedor de serviços de internet a responsabilidade objetiva, conforme previsto na Lei de Direitos Autorais (Lei nº 9.610/98), de modo o que o provedor será responsabilizado, sem necessidade de comprovação de culpa, caso não remova o conteúdo publicado por terceiros após notificação extrajudicial (parágrafo 2º do artigo 19 da Lei n.º 12.965/14) (Souza; Lemos, 2016).

A outra exceção diz respeito a pública de pornografia de vingança[6]: quando notificado extrajudicialmente, o provedor deve remover o conteúdo de "pornografia de vingança" para evitar responsabilização pelos danos causados à vítima (art. 21 da Lei n.º 12.965/14):

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo (Brasil, 2014).

[6] A pornografia de vingança refere-se à prática de compartilhar, na internet, imagens ou vídeos íntimos de terceiros sem o consentimento destes, mesmo que tenham sido capturados em momentos privados, sem a intenção de divulgação pública.

Em contrapartida, o entendimento jurisprudencial tem ido de encontro ao Marco Civil da Internet, uma vez que, em alguns casos, tem-se utilizado a aplicação do Código de Defesa do Consumidor em favor da vítima, atribuindo ao provedor a responsabilidade objetiva. A seguir, são apresentados trechos do fundamento utilizado na decisão de segunda instância que imputou a responsabilidade ao provedor de aplicações:

> Recurso Extraordinário nº 1.037.396/SP: Para fins indenizatórios, todavia, condicionar a retirada do perfil falso somente após ordem judicial específica, na dicção desse artigo, significaria isentar os provedores de aplicações, caso da ré, de toda e qualquer responsabilidade indenizatória, fazendo letra morta do sistema protetivo haurido à luz do Código de Defesa do Consumidor, circunstância que, inclusive, aviltaria preceito constitucional (art. 5º, inciso XXXII, da Constituição Federal).
> Ademais, tal disposição como que quer obrigar, compelir o consumidor vitimado, a ingressar em Juízo para atendimento da pretensão que, seguramente, poderia ser levada a cabo pelo próprio provedor cercando-se de garantias a fim de preservar, em última análise, a liberdade de expressão. Antes, o provedor fica em confortável, mas não menos desproporcional, posição de inércia frente à vítima do abuso desse mesmo direito de manifestação e pensamento, gerando paradoxal desequilíbrio em relação aos invioláveis direitos à intimidade, à vida privada, a honra e à imagem (art. 5º, inciso X, da Constituição Federal) desta última (vítima).
> Inegável que na relação entre as litigantes a autora, diante de sua notória condição de vítima, equipara-se à figura do consumidor (art. 17 do Código de Defesa do Consumidor). […].
> Destarte, condicionar a responsabilização da ré à prévia tomada de medida judicial pela autora, na conformidade do art. 19 do Marco Civil da Internet, fulminaria seu direito básico de efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos (art. 6º, inciso VI, do Código de Defesa do Consumidor). Logo, a indenização pelos danos morais é medida que se impõe [...]. (Brasil, 2018).

No caso em questão, a vítima alegou em sua defesa que o artigo 19 do Marco Civil da Internet é lesivo ao direito básico do consumidor, de modo que o referido dispositivo promove a inércia dos provedores em face da parte que sofreu violação da intimidade, vida privada, honra e imagem, sendo incompatível com o artigo 5º, inciso X, da Constituição Federal.

Inobstante isso, o Supremo Tribunal Federal discute, através do Recurso Extraordinário 1.037.396, a constitucionalidade do art. 19, do Marco Civil da Internet, no que diz respeito à necessidade de ordem judicial para que haja exclusão de conteúdo ilícito, de forma prévia, sob pena de responsabilização civil do provedor (Processo sob Repercussão Geral n° 987/STF).

O RE 1.037.396 trata sobre um agente que criou um perfil falso na rede social Facebook, e desferiu ofensas ao ofendido. O Tribunal de primeira instância ordenou a remoção do perfil falso e também solicitou a divulgação do endereço IP do responsável pelas ofensas. Contudo, concluiu que não existia obrigação de indenização por parte da plataforma de mídia social. Essa conclusão se baseou no fato de que, no caso específico, não havia uma

ordem judicial explicitando a necessidade de eliminar o conteúdo. Portanto, de acordo com o artigo 19 do Marco Civil da Internet, o Tribunal de origem determinou a ausência da obrigação de indenizar. No contexto do Supremo Tribunal Federal, a ex-Ministra Ellen Gracie ressaltou:

> A responsabilidade civil dos provedores de aplicação de internet (...). Veja-se: "Tema 533 - Dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário (relator ministro Luiz Fux, RE 1.057.258)". O segundo caso é o Tema 987, citado acima, que ainda está pendente de decisão. Veja-se: "Tema 987 - Discussão sobre a constitucionalidade do artigo 19 da Lei 12.965/2014 (Marco Civil da Internet) que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros (...)". Antes da Lei do Marco Civil, (...) todo dano deveria ser ressarcido pelos provedores de aplicação que não atendessem à solicitação do lesado, bastando que o usuário noticiasse a ocorrência do incidente, por intermédio do próprio serviço (provedor de aplicação), solicitando a remoção imediata do conteúdo. A partir do Marco Civil, a responsabilização do provedor de aplicação por não remoção do conteúdo passa a depender de decisão judicial específica e fundamentada (...) (Brasil, 2020).

Antes da promulgação da Lei do Marco Civil, qualquer dano deveria ser ressarcido pelos provedores de aplicação que não atendessem à solicitação do lesado. Bastava que o usuário notificasse a ocorrência do incidente por meio do próprio serviço (provedor de aplicação), solicitando a remoção imediata do conteúdo. No entanto, com a entrada em vigor do Marco Civil, a responsabilização do provedor de aplicação por não remoção do conteúdo passa a depender de uma decisão judicial específica e fundamentada, como ressaltado no texto referente ao ano de 2020 no Brasil.

2.4 A INFORMAÇÃO E A DESINFORMAÇÃO NA ERA DIGITAL A PARTIR DE ALGUNS CASOS DE *DEEPFAKE*

Na era digital, a informação e a desinformação desempenham papéis cruciais, influenciando a sociedade, a política, a economia e a cultura de maneiras sem precedentes. Com o advento de novas tecnologias, como a *deepfake*, essa capacidade atinge níveis inimagináveis.

Como a tecnologia de *deepfake* permite a criação de vídeos e áudios falsificados extremamente convincentes, o seu potencial de difamar pessoas públicas, espalhar informações falsas e desacreditar fontes confiáveis, pode acabar minando a confiança na informação.

No pleito eleitoral de 2022, começou a circular nas redes sociais, principalmente no Whatsapp, um vídeo adulterado do Jornal Nacional, principal noticiário do Brasil, com o

intuito de desinformar eleitores. Na mídia, amplamente divulgada, os âncoras William Bonner e Renata Vasconcellos divulgavam o resultado de uma pesquisa de intenção de votos para a presidência (Ipec) apontando o candidato Jair Bolsonaro à frente dos demais. Contudo, essa informação era falsa. Tanto os dados e gráficos estavam invertidos, quanto as falas dos apresentadores (Nacional, 2022).

Na verdade, as pesquisas do Ipec e do Datafolha, apresentadas no Jornal Nacional desde 15 de agosto de 2022, o candidato do PT, Luiz Inácio Lula da Silva, foi consistentemente indicado como o líder em intenções de voto. Em todas essas pesquisas, Bolsonaro ficou em segundo lugar (Nacional, 2022).

Após o ocorrido, o telejornal fez um pronunciamento com o objetivo de alertar aos telespectadores que o vídeo foi usado com o intuito de espalhar desinformação para a sociedade, afirmando que se tratava da utilização de *deepfake*, técnica que emprega inteligência artificial para realizar modificações substanciais no conteúdo, uma vez que por meio dessa técnica, torna-se viável realizar substituições digitais do rosto de uma pessoa ou simular sua voz, levando a representações de ações ou falas que a pessoa não realizou ou disse (Schmidt, 2022). Na época, o Deputado Federal, Guilherme Boulos, escreveu em sua conta no Twitter que:

> Desde ontem, circula pelas redes sociais um vídeo "*deepfake*" com o Jornal Nacional dizendo que o miliciano ultrapassou Lula nas pesquisas. De qual computador saiu a 1ª postagem? Tem empresários financiando? A hora de colocar o gabinete do ódio e o golpismo na cadeia é agora! (Boulos, 2022).

Outro vídeo do telejornal que apresentava uma edição semelhante, manipulando os resultados de uma pesquisa presidencial. Dessa vez, o vídeo foi compartilhado no TikTok, atingindo 2,5 milhões de visualizações. A informação foi confirmada pelo Projeto Comprova, uma iniciativa que conta com jornalistas de 43 veículos de comunicação no Brasil para verificar a desinformação (Schmidt, 2022). Nessa mesma rede social foi publicado um outro vídeo onde o apresentador do Jornal Nacional, William Bonner, chamava o candidato Luiz Inácio Lula da Silva de ladrão. No entanto, a voz que foi atribuída a Bonner foi, na verdade, gerada de forma sintética a partir de um texto (Ninja, 2022).

Após o início da guerra entre Rússia e Ucrânia, um vídeo do presidente ucraniano, Volodymyr Zelensky, circulou nas redes sociais, pedindo aos compatriotas que se rendessem à Rússia, baixassem as armas e regressassem para suas casas. Contudo, o vídeo se trata de mais uma *deepfake*. O próprio Zelensky desmentiu o conteúdo em sua conta oficial no Instagram.

Nas imagens, o rosto do presidente estava sobreposto a um corpo com movimentos mínimos, usando uma camiseta verde.

Na China, um caso de fraude acendeu o alerta sobre o perigo das *deepfakes*. A polícia constatou que, a partir da utilização dessa inteligência artificial, um homem foi convencido a realizar uma transferência no valor de US$622 mil para um suposto amigo durante uma chamada de vídeo (Spadoni, 2023).

Segundo Pedro Spadoni (2023), a vítima acreditou que estava transferindo a quantia em dinheiro para o seu amigo, que na situação precisava fazer um depósito em face de um processo licitatório. Contudo, só percebeu que havia caído em uma *deepfake* quando seu amigo real negou conhecimento sobre o que ele estava mencionando, conforme foi explicado pelas autoridades locais através de comunicado à imprensa. A vítima conseguiu recuperar a maior parte do dinheiro que foi roubado e, atualmente, está empenhada em rastrear o restante.

O empresário Elon Musk teve seu rosto utilizado para a replicação de vídeos criados através da *deepfake*. Os criminosos tinham por objetivo subtrair dinheiro de investidores de criptomoedas. Para dar uma aparência mais autêntica ao golpe, a plataforma de criptomoedas chamada BitVex enfatizava que o bilionário era o presidente-executivo, e ainda prometia um lucro de 30% após os investimentos (Mannara, 2022).

A escolha do empresário, que também é proprietário da SpaceX (empresa aeroespacial), deve-se ao fato de ele ser um grande entusiasta das criptomoedas. Muitos de seus *tweets* abordam comentários sobre o Bitcoin, uma das criptomoedas mais conhecidas. Além disso, o valor da "moeda meme" chamada Dogecoin, criada a partir de uma imagem de um cachorro da raça Shiba Inu, disparou após o apoio do bilionário. Em uma postagem em uma rede social, ele chegou a mencionar que a Tesla aceitaria Dogecoin como forma de pagamento (Mannara, 2022).

O golpe envolvendo a Bitvex foi mais elaborado do que simplesmente usar a imagem de Elon Musk. Canais do YouTube que abordavam temas relacionados ao mundo digital ou criptomoedas foram alvo de invasões. Os invasores começaram a publicar vídeos promovendo a plataforma Bitvex, buscando atrair um maior número de vítimas (Mannara, 2022).

Outro caso que revela o perigo das *deepfakes*, ocorreu no estado norte-americano da Pennsylvania. Uma mulher, chamada Raffaela Spone, de 50 anos, foi presa após ter criado fotografias inverídicas de jovens nuas, fumando ou bebendo. Essas imagens eram enviadas para os responsáveis pela equipe de torcida com a finalidade de que as meninas fossem expulsas do time, em favorecimento da sua filha. Além disso, Spone enviava as fotos para as próprias vítimas, estimulando-as ao suicídio (Rigues, 2021).

Em julho de 2021, a polícia local recebeu a primeira denúncia. Na ocasião, a partir das mensagens que uma das vítimas recebeu através de um número anônimo, a polícia iniciou, por mandados de busca, o rastreamento dos números e chegaram num site de ferramentas de telemarketing que entregou o endereço IP do remetente, que os levou à Spone. Após uma varredura no celular da suspeita, foram encontradas evidências dos crimes cometidos. A mesma encontrava-se enfrentando três acusações de assédio e três de assédio cibernético contra menor.

George Ratel, pai de uma das vítimas, acredita que Spone começou o assédio moral depois que ele e sua esposa pediram à sua filha para interromper o relacionamento com a garota, devido à preocupação quanto ao comportamento dela.

Dada a crescente complexidade resultante do avanço tecnológico na disseminação de informações (e desinformação) no meio virtual, é crucial ressaltar a necessidade de ferramentas jurídicas para estabelecer formas de responsabilização, especialmente no âmbito criminal, na busca pelo combate e prevenção de crimes de desinformação através das redes sociais.

3 AS ATUAIS FERRAMENTAS JURÍDICAS DE COMBATE E PREVENÇÃO À DESINFORMAÇÃO ON-LINE

O capítulo anterior debruçou-se sobre a relação entre a era digital e a tutela jurídica do direito à informação, considerando a complexidade da *deepfake* empregada às fake news, assim como sua responsabilização civil. Agora, ao adentrar no terceiro capítulo, observa-se as ferramentas jurídicas atuais para combater e prevenir a desinformação on-line no âmbito criminal.

3.1 O COMBATE E A PREVENÇÃO ÀS *DEEPFAKES* E ÀS FAKES NEWS NO DIREITO COMPARADO

No âmbito do direito, ainda predomina a ausência de legislação que trate sobre a utilização da *deepfake* para disseminar desinformação, tanto no Brasil, quanto em outros países. Apesar disso, no ordenamento jurídico internacional existem alguns modelos de medidas empregadas para reprimir o avanço desenfreado de novas tecnologias, conquanto a ausência generalizada de leis específicas sobre o uso de *deepfake*, principalmente na propagação de notícias falsas, é importante abordar as questões jurídicas pertinentes, considerando as potenciais implicações negativas que podem ter na sociedade.

No direito comparado, há alguns exemplos de medidas que foram tomadas para tentar frear esse avanço desordenado das novas tecnologias, mesmo com o vácuo legislativo generalizado quanto a *deepfake*, já que elas podem trazer possíveis repercussões negativas para a sociedade.

Na Malásia, um incidente peculiar ocorreu relacionado à implementação de uma legislação pioneira para combater a disseminação de desinformação, particularmente no contexto político. Neste caso, a prática de espalhar informações incorretas foi estabelecida como um crime sujeito a uma pena de até seis anos de prisão. Contudo, essa lei foi posteriormente considerada excessivamente prejudicial, levando à revogação em agosto de 2018 (Pinto, 2019).

A China implementou novas regulamentações para conteúdos escritos, em vídeo e áudio on-line, exigindo que qualquer modificação feita por Inteligência Artificial ou Realidade Virtual seja claramente identificada. Além disso, as regras incluem a proibição da disseminação de notícias falsas produzidas por meio de *deepfakes*. Estas diretrizes foram

elaboradas pela Administração do Ciberespaço da China (CAC). O não cumprimento dessas regras é considerado uma ofensa criminal (Raupp, 2019).

Conforme a nova legislação formulada pela Administração do Ciberespaço da China, tanto os provedores de tecnologia relacionados a *deepfakes* quanto os usuários são passíveis de responsabilidade pela divulgação de informações falsas. É exigido que obtenham consentimento explícito dos usuários antes de realizar qualquer manipulação de vídeos e/ou imagens. A utilização de Inteligência Artificial sem a devida identificação está proibida, e atividades ilegais que empreguem IA sem essa identificação são estritamente restringidas. Além disso, as empresas que oferecem serviços em plataformas de redes sociais devem estabelecer sistemas para contestar e desmentir boatos (Reina, 2023).

Os principais regulamentos para o espaço cibernético chinês visam restringir atos inadequados e prevenir a prática de crimes, em conformidade com a estrutura jurídica vigente no país. No entanto, a nova regulamentação ainda não estabelece medidas punitivas específicas para quem violar as normas. As penalidades aplicáveis serão determinadas com base na legislação já em vigor nas áreas de segurança de rede, comércio eletrônico, segurança de dados e proteção de informações pessoais (Reina, 2023).

Nos Estados Unidos, em que pese a tramitação inúmeros projetos de lei acerca da *deepfake*, alguns Estados criaram leis específicas com a finalidade de regulamentar e combater tal fenômeno. No estado da Califórnia, uma lei foi promulgada em 2019, tornando ilegal a criação ou distribuição de *deepfakes* dentro de sessenta dias após uma eleição. O objetivo principal dessa legislação é prevenir a manipulação enganosa de conteúdo com o propósito de enganar eleitores ou prejudicar candidatos no âmbito político (Viçozo, 2021).

Além disso, o estado da Virgínia também buscou tratar sobre o referido tema ao estabelecer, no ano de 2019, uma lei que criminaliza a conduta de pornogafia de vingança, bem como seu compartilhamento nos mais variados meios. Através da atualização de uma lei já vigente, a Virgínia atribuiu a utilização de *deepfake* a ato criminoso, ao incluir fotos e vídeos manipulados por essa tecnologia. Nesse passo, a legislação classifica essa infração como uma contravenção de “classe 1”, sujeita a uma pena de até doze meses de prisão ou uma multa que pode chegar a 2,5 mil dólares (Raupp, 2019).

No âmbito nacional nos Estados Unidos, as discussões sobre a utilização de *deepfake* na desinformação foram bloqueadas no Congresso em 2021, com a alegação de cerceamento da liberdade de expressão. Enquanto isso, na Europa, o debate sobre o assunto ainda está em curso. A União Europeia está trabalhando com a recomendação de que as próprias

plataformas desenvolvam meios para evitar o uso de *deepfakes* na propagação de desinformação (Reina, 2023).

Nesse contexto, é perceptível que no Estado Democrático de Direito, a ausência de leis que regulam o exercício das liberdades pode resultar em uma fragmentação do Estado, com disposições políticas arbitrárias e inconsistentes.

3.2 O COMBATE E A PREVENÇÃO ÀS *DEEPFAKES* E ÀS FAKES NEWS NO ORDENAMENTO JURÍDICO BRASILEIRO

Atualmente, como uma medida brasileira para enfrentar a propagação de notícias falsas e *deepfakes*, destaca-se o Marco Civil da Internet. Esse marco foi estabelecido por meio da Lei n.º 12.965/14, a qual define princípios, garantias, direitos e deveres para a utilização da Internet no Brasil, conforme discussão apresentada no capítulo anterior.

Além disso, segundo o Código Civil, configura-se um ato ilícito quando alguém, por omissão ou ação voluntária, negligência ou imprudência, viola o direito de outrem. Em outras palavras, aquele que, de forma intencional, por negligência ou imprudência, divulgar informações falsas sobre uma pessoa a ponto de causar danos materiais ou morais, estará sujeito à obrigação de reparação (Brasil, 2002).

Nesse contexto, encontra-se atualmente em discussão o Projeto de Lei nº 2.630/2020, que tem por objetivo regulamentar o uso das plataformas on-line no que tange a produção e disseminação de notícias falsas, como será abordado mais detalhadamente a seguir.

3.2.1 O projeto de Lei. 2.630/2020: O PL das fake news

O Projeto de Lei n.º 2.630 de 2020, popularmente conhecido como “PL das Fake news”, institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet e, foi apresentado pelo Senador Alessandro Vieira (Cidadania – SE), inicialmente, com o objetivo de combater à escalada da desinformação no âmbito virtual (Brasil, 2020).

Após alguns anos de processo de elaboração, o projeto vem revelando suas ambivalências. Ele inclui a tentativa de regulamentar certos aspectos do uso da internet, com o objetivo de restringir as atividades comerciais das plataformas, especialmente das empresas de porte médio e pequeno que atuam no ambiente digital. Além disso, propõe estabelecer diretrizes questionáveis para controlar o comportamento dos usuários, impulsionar propaganda político-eleitoral e até mesmo abordar questões de natureza criminal (Conjur, 2021).

Barros e Oliveira (2021) destacam que a harmonização entre esses dois parâmetros está estreitamente ligada à responsabilidade legal atribuída aos intermediários, particularmente nas redes sociais. Existe uma escala de responsabilidade que varia desde a ausência total de responsabilidade pelo conteúdo veiculado, em que não há incentivo para intervenção, e qualquer remoção de conteúdo depende de uma ordem oficial (modelo adotado nos Estados Unidos); até a consagração de uma imunidade condicional, na qual o moderador deve seguir procedimentos pré-estabelecidos, como notificar a parte interessada e remover o conteúdo, ou ainda fornecer aviso e notificação sobre a solicitação de terceiros para remover o conteúdo. Ainda, há a responsabilidade integral, na qual os intermediários são responsáveis por todo o conteúdo divulgado em suas plataformas. Neste caso, é permitido o monitoramento e a pronta remoção de conteúdos que possam gerar responsabilização.

Apesar do projeto de lei em questão, de alguma forma, restringir certas liberdades individuais, como a liberdade de expressão, é imperativo ressaltar a importância da sua regulamentação, uma vez que a ausência de regulamentação tem acarretado consequências perceptíveis em todo o país, levando a uma sociedade constantemente alerta diante de uma enxurrada de desinformações. Barros e Oliveira (2021, p. 01) defendem a necessidade premente de uma legislação que atenda aos anseios da dignidade social, especialmente diante do impacto das *fake news*, com a finalidade de mitigar os efeitos negativos e preservar a integridade das informações, ainda mais com advento de novas tecnologias, como a *deepfake*, vejamos:

> É absolutamente fundamental o desenvolvimento e aplicação de critérios transparentes e objetivos de remoção algorítmica de notícias, de forma a garantir, mais que tratamento equânime e impessoal a todos os indivíduos/ideologias, o prévio conhecimento e potencial controle dos motivos e circunstâncias ensejadoras da remoção de conteúdo. Imprescindível, ainda, o envolvimento da sociedade civil com vistas ao combate e impulsionamento de notícias capazes de desmentir as falsas — estratégia comprovadamente eficaz, conforme se vê da pesquisa levada a efeito pela Fundação Getúlio Vargas com relação às inverdades propagadas na rede quanto à morte da vereadora Marielle Franco e a reação voltada à sua desconstrução, que atingiu vulto e alcance muitíssimo maiores a partir de uma mobilização popular concisa e efetiva.

Nesta conjuntura, o PL n.º 2.630 de 2020 traz em seu texto normas, diretrizes e mecanismos acerca da transparência nas redes sociais e serviços de mensageria privada por meio da internet, que seja capaz induzir ao abuso ou manipulação da sociedade. Em outras palavras, o PL visa combater a proliferação de notícias falsas nas mídias digitais, como Instagram, WhatsApp, Twitter, Telegram e outros. Em contrapartida, em consonância com o disposto no Art. 2º da referida lei, esta somente se aplica aos provedores de aplicativos que

exerçam atividade organizada e, cujo público seja superior a dez milhões de usuários registrados.

A legislação proposta não irá impor penalidades a empresas envolvidas em atividades específicas, tais como comércio eletrônico (e-commerce), plataformas para reuniões por vídeo ou voz (como o aplicativo Zoom), enciclopédias online sem fins lucrativos, jogos e apostas on-line, ou repositórios científicos, educativos e de dados do Poder Público, entre outros exemplos.

No artigo quarto do Projeto de Lei, são apresentados os objetivos essenciais, salientando o fortalecimento do processo democrático por meio do combate à disseminação de desinformação e do estímulo à diversidade de informações na internet no Brasil. O texto propõe buscar uma maior transparência em relação a sua atividade com os usuários e incentivar um ambiente cibernético saudável, visando garantir um espaço virtual seguro e livre de desinformação.

> Art. 4º Essa Lei tem como objetivos:
> I – o fortalecimento do processo democrático e o fomento à diversidade de informações no Brasil;
> II – a garantia da transparência dos provedores em relação a suas atividades com o usuário, incluindo a elaboração e modificação de seus termos de uso, critérios de moderação e recomendação de conteúdos e identificação de conteúdos publicitários;
> III – o exercício do direito do usuário à notificação, ao contraditório, ampla defesa e devido processo em relação à moderação de conteúdos;
> IV – o fomento à educação para o uso seguro, consciente e responsável da internet como instrumento para o exercício da cidadania;
> V – proteção integral e prioritária dos direitos fundamentais das crianças e adolescentes; e
> VI – o incentivo a um ambiente livre de assédio e discriminações. A. (Brasil, 2020).

A atuação dos provedores de redes sociais deve incidir, firmemente, no combate e na prevenção às práticas ilícitas dentro de suas plataformas, assim que receberem uma notificação acerca de conteúdos com potencial criminoso. Dentre os exemplos de conteúdo que pode ser considerados ilegal e passíevis de penalização, o art. 11 do PL das Fake news, traz em seu rol: a) Crimes contra o Estado Democrático de Direito; b) Atos de terrorismo e planejamento de terrorismo; c) Estímulos ao suicídio e à automutilação; d) Crimes contra crianças e adolescentes; e) Práticas de crimes de racismo; f) Violência contra a mulher; g) Dificultar ou contrariar medidas sanitárias em caso de decreto de situação de emergência em saúde pública, sendo considerado uma infração sanitária.

Além de prevenir e combater esses conteúdos, é necessário evitar a disseminação em larga escala dessas publicações. O projeto de lei sobre desinformação também prevê que as

plataformas devem avaliar os riscos sistêmicos de seus serviços, os quais podem estar facilitando a propagação de conteúdo ilegal, ou até mesmo ameaçando a liberdade de expressão. Essa avaliação inclui: a) Sistemas de recomendação e outros algoritmos; b) Sistemas de moderação de conteúdos; c) Termos de uso e sua aplicação; d) Sistemas de exibição de anúncios publicitários; e) Aberturas no sistema que possibilitem a manipulação de forma intencional, como é o exemplo da criação de contas falsas (Brasil, 2020).

Os documentos de registro das análises precisam ser publicados, pelo menos, uma vez ao ano ou sempre que houver alteração significativa nas plataformas. Os relatórios, deverão, obrigatoriamente, conter: números de usuários, alterações realizadas no serviço, procedimentos de moderação, conteúdos proibidos e parâmetros que guiam a recomendação ou exibição de conteúdo.

No que concerne à responsabilidade dos provedores de aplicação na luta contra a desinformação e na promoção da transparência na internet, através da moderação de conteúdos publicados na internet, o projeto de lei delineia em suas disposições gerais, especialmente no seu artigo 13, o seguinte:

> Art. 13. A partir da instauração do protocolo de segurança e devida notificação, os provedores poderão ser responsabilizados civilmente pelos danos decorrentes de conteúdo gerado por terceiros quando demonstrado conhecimento prévio, nos termos do art. 16.
> Parágrafo único. A responsabilidade dos provedores por danos decorrentes de conteúdo gerado por terceiros, quando houver risco iminente de danos, será solidária, incidirá pelo período de duração do protocolo e será restrita aos temas e hipóteses nele estipulados (Brasil, 2020).

Nesse contexto, entende-se que todos os envolvidos podem ser responsabilizados conjuntamente, garantindo uma responsabilidade mais ampla para os provedores no que diz respeito aos danos causados por conteúdos gerados por terceiros, quando há prévio conhecimento e risco iminente.

Além disso, as plataformas serão obrigadas a restringir contas automatizadas ou geridas por robôs que não se identificam como tal para os usuários. Para evitar esse tipo de conta, os serviços terão que implementar medidas para identificar aquelas que demonstram atividade incompatível com a capacidade humana. Além disso, devem estabelecer políticas de uso que limitem o número de contas controladas por um mesmo usuário (Haje, 2020).

Tais medidas revelam-se imensamente importantes, uma vez que, hodiernamente, há empresas que fornecem essa forma de serviço, de modo que qualquer indivíduo pode ofertar, vender e manipular perfis, com a finalidade de propagar notícias fraudulentas. Na situação de publicação de conteúdos patrocinados, a lei requer a identificação dos usuários. Isso serviria

como uma medida para prevenir anúncios enganosos relacionados a golpes financeiros (Sérvio, 2022).

Outra medida importante para o combate às notícias falsas, principalmente com o uso de *deepfake*, trazida na lei, diz respeito à limitação do número de encaminhamentos de mensagens e mídias, por parte das empresas que prestam o serviço de mensageria privada. Adicionalmente, os provedores de aplicação devem permitir que os usuários decidam se desejam ou não participar de grupos de mensagens e listas de transmissão. Inclusive, os provedores de serviços de mensagens instantâneas devem desenvolver soluções para identificar e impedir mecanismos externos de distribuição em grande escala, conforme descrito no artigo 41.

Portanto, em situações que seja necessário a aplicação de regra prevista nos termos de uso, os usuários devem receber notificações com o detalhamento da razão, do processo de análise e da execução da medida, assegurado o direito de contestação. O usuário terá o direito de resposta com a mesma extensão do conteúdo considerado inadequado.

No que se refere à publicidade, todos os conteúdos patrocinados presentes nas plataformas digitais devem ser identificados, possibilitando que os usuários tenham a oportunidade de entrar em contato com os anunciantes, conforme especificado no artigo 26 do texto legal: "Art. 26. Os provedores que ofereçam publicidade de plataforma devem identificá-la, de modo que o usuário responsável pelo impulsionamento ou o anunciante sejam identificados" (Brasil, 2020).

De mais a mais, o texto da lei traz também responsabilidades relativas à Administração Pública. Em conformidade com o art. 33, as contas de agentes políticos, que ocupam mandatos eletivos, são de interesse público. Desse modo, estão sujeitas às contas oficiais de vereadores, deputados, senadores, etc., além de outros cargos de gestão de órgãos públicos diretos e indiretos (Coelho, 2020).

Em contrapartida, essas contas oficiais ficam impossibilitadas de limitar o acesso de outras contas às suas postagens (art. 33, §1º). Além do mais, se o agente tiver duas ou mais contas numa mesma plataforma, ele poderá escolher qual conta que representa seu mandato ou cargo, de modo que as outras serão dispensadas dos preceitos da lei.

Outrossim, está prevista a implementação de um sistema de auto-regulamentação das plataformas, sob a supervisão do Comitê Gestor da Internet (CGI.br). O relator destaca que esse modelo é considerado superior à criação do Conselho de Transparência e Responsabilidade na Internet, proposto no texto do Senado. Segundo o relator, essa decisão se

embasa no fato de o CGI já possuir expertise e experiência consolidada em regulamentações relacionadas à internet (Conjur, 2021).

No que se refere às sanções e punições, a nova legislação, na hipótese negligência ou falta de adoção de medidas suficientes, por parte das plataformas, para combater conteúdos ilegais diante de "risco iminente de danos", sendo considerada a implementação de um protocolo de segurança com uma duração inicial de 30 dias, com possibilidade de prorrogação (Conjur, 2021).

Nesse contexto, as plataformas poderão ser responsabilizadas por conteúdo criado por terceiros, como cidadãos comuns, por exemplo. Contudo, é necessário a comprovação de que a plataforma tinha conhecimento prévio sobre a ilicitude do conteúdo e, mesmo assim, optaram pela omissão no caso. Considera-se "conhecimento prévio" o conteúdo que tenha sido denunciado por usuários da plataforma, de modo que os provedores são incumbidos de estabelecer mecanismos para receber denúncias.

O PL n.º 2.630 de 2020 prevê sanções e/ou punições, também, nas situações de abuso de moderação pelo cumprimento das exigências, sendo cabíveis ao descumprimento da lei as seguintes punições: a) Advertência, oferecendo um prazo para que a plataforma possa agir sobre o conteúdo; b) Multas, podendo chegar a R$50 milhões de reais por infração e; c) Suspensão ou proibição das atividades no país. Ademais, para indivíduos que promoverem ou financiarem a disseminação em larga escala de notícias falsas, está prevista a possibilidade de uma pena que varia de um a três anos de prisão, além do pagamento de multa.

Em síntese, observa-se que a possível legislação busca regularizar o direito à informação e a liberdade de expressão sob o princípio basilar da democracia difundido no país. É evidente que não há violação desses direitos, apenas a sua regulação.

3.3 INTERVENÇÃO DO DIREITO PENAL NA TUTELA DOS BENS JURÍDICOS AFETADOS PELAS *FAKE NEWS*

No direito brasileiro, até a presente data desta monografia, processa-se a inexistência de ordenamento jurídico-penal de um tipo penal incriminador para a produção de compartilhamento de notícias fraudulentas, com a respectiva pena a ser aplicada àquele que incorrer na referida conduta.

Em consonância com os ensinamentos de Bitencourt (2020), o Direito Penal refere-se à violência de direitos e/ou interesses individuais dos cidadãos. Assim, o Direito Penal, ciência autônoma e com natureza intrinsecamente de controle social, surge nas situações que a

violação de direitos adquire proporções que outros ramos do direito são incapazes de manter/trazer de volta a harmonia e controle social. Disserta Bitencourt (2020, apud Puig, 2010, p. 57) que:

> O Direito Penal apresenta-se, por um lado, como um conjunto de normas jurídicas que tem por objeto a determinação de infrações de natureza penal e suas sanções correspondentes — penas e medidas de segurança. Por outro lado, apresenta-se como um conjunto de valorações e princípios que orientam a própria aplicação e interpretação das normas penais.

Nesse contexto, o Direito Penal se diferencia dos outros ramos do direito em detrimento de sua característica fracionária, uma vez que ele representa a última *ratio* do sistema para a égide dos bens jurídicos de maior relevância para os cidadãos e sociedade (Bitencourt, 2020).

Portanto, o Direito Penal visa a proteger bens jurídicos mais valiosos para os cidadãos, como por exemplo: a vida, a liberdade, a honra, o patrimônio, a segurança, dentre outros. Nessa esteira, "o bem se apresenta vinculado aos mais preciosos interesses humanos, seja do ponto de vista material, seja do prisma incorpóreo (moral ou ético)" (Nucci, 2020, p. 30). Ainda nesse pensamento, Guilherme Nucci (2020, p. 51) destaca que:

> Há bens tutelados pelo Direito, eleitos pelo ordenamento jurídico como indispensáveis à vida em sociedade, merecendo proteção e cuidado. A partir dessa escolha, o bem se transforma em bem jurídico. Dos mais simples aos mais complexos; dos inerentes à natureza humana às criações alternativas da vida moderna; dos ligados à dignidade humana aos vinculados a puros interesses materialistas; todos os bens jurídicos gozam do amparo do Direito. Os mais relevantes e preciosos atingem a tutela do Direito Penal, sob a ótica da intervenção mínima.

Devido ao fato de lidar com os bens jurídicos mais essenciais para os indivíduos e a sociedade, impondo sanções mais severas àqueles que os infringem, o Direito Penal se baseia, entre outros princípios, na estrita legalidade. Esse princípio determina que não existe crime sem uma lei anterior que o defina, nem pena sem previsão legal, sendo refletido no texto constitucional pelo artigo 5°, inciso XXXIX (Brasil, 1988). Sendo assim, a conduta que não se encontra tipificada no ordenamento jurídico penal, ou que inexista pena previamente instituída, é imperativo concordar que não existe crime.

Nessa perspectiva, entende-se que o tipo penal não apenas estabelece uma seleção de condutas, mas também implica uma valoração, pressupondo que o comportamento tipificado já é inerentemente relevante no âmbito penal. No entanto, é válido ressaltar que certas condutas, embora se enquadrem nos tipos penais, podem carecer de relevância por serem consideradas comuns ou aceitas no contexto social. Isso ocorre devido ao frequentemente

existente desalinhamento entre as normas penais incriminadoras e aquilo que é socialmente permitido ou tolerado (Bitencourt, 2018).

A prática de um crime será determinada, fora os diversos aspectos cruciais para o texto legal e ao processo legislativo apropriado, a partir da insuficiência ou ineficácia de outros ramos do direito para proteger assentado bem jurídico. Ademais, não são todos os bens jurídicos que precisam ser protegidos pelo Direito Penal, uma vez que "segundo o princípio da intervenção mínima, são reservados os mais relevantes bens jurídicos, focando-se as mais arriscadas condutas, que possam, efetivamente, gerar dano ou perda ao bem tutelado", assim, quanto maior a importância do bem jurídico violados, maior gravidade das penas impostas (Nucci, 2020).

> O bem escolhido pelo ordenamento jurídico para ser tutelado e amparado. Quando se constituir em bem jurídico deveras relevante, passa ao âmbito de proteção penal, permitindo a formação de tipos incriminadores, coibindo as condutas potencialmente lesivas ao referido bem jurídico penal. (Nucci, 2020, p. 18).

O entendimento sobre os bens jurídicos protegidos pelo Direito Penal é fundamental, porquanto, em conformidade com o que disserta Cezar Roberto Bitencourt (2020), "o conceito de bem jurídico está relacionado à finalidade de preservação das condições individuais necessárias para uma coexistência livre e pacífica em sociedade, garantindo, ao mesmo tempo, o respeito de todos os direitos humano", desse modo "como o ponto de partida da estrutura do delito é o tipo de injusto, este representa a lesão ou perigo de lesão do bem juridicamente protegido".

Quando se trata da aplicação da lei penal a atividades ilícitas realizadas no espaço cibernético, emerge um desafio em potencial devido ao fato do Código Penal Brasileiro, elaborado em 1940, não ter contemplado explicitamente tipos penais destinados a lidar com transgressões presentes na contemporaneidade, como a disseminação de notícias falsas (Martin, 2019).

Tiago Caruso (2021), assevera que um dos maiores empecilhos para criminalizar as fake news (a partir da produção e compartilhamento na internet) é justamente a especificação do bem jurídico em risco por essa conduta que merece a salvaguarda do ordenamento jurídico penal.

> Há quem entenda tratar-se da proteção das instituições democráticas, posição aqui compartilhada, justamente porque constitui princípio fundamental da República Federativa do Brasil (art. 1º, CF). Outros, entendem que se trata de proteger a liberdade de informação, a verdade ou, ainda, aspectos eleitorais,(20) como a liberdade para a formação do voto.(21) Partindo da ideia de que as fake news violam as instituições democráticas – ou ainda, a liberdade de informação ou de formação do voto –, parece haver determinação de ofensa a bem jurídico com dignidade penal,

> atendimento ao princípio da subsidiariedade, pois tais bens jurídicos ainda não possuem tutela penal adequada, e da fragmentariedade, uma vez que apenas a difusão dolosa de notícias falsas, com finalidade de desinformar para proveito próprio ou alheio, seria objeto de criminalização. Contudo, esses são apenas os primeiros obstáculos para a criminalização das fake news. Ultrapassados, outros surgem e se referem à observância aos princípios que norteiam o Direito Penal, como a taxatividade, a pessoalidade, a culpabilidade e a proporcionalidade.(22) A tarefa não é fácil, nem deve ser, pois o Direito Penal sempre lida com um dos valores mais caros da vida em sociedade, que é a liberdade do indivíduo (Caruso, 2021, on-line).

No âmbito da desinformação, o Código Penal deve proteger a honra dos cidadãos, mas também a possível vulnerabilidade deles diante de notícias divulgadas de má-fé, principalmente se utilizada tecnologia de *deepfake*. Conforme a visão de Fernando Capez (2019, p. 91), a perspectiva do Direito Penal deve ser fundamentada no risco concreto:

> Não há crime quando a conduta não tiver oferecido ao menos um perigo concreto, real, efetivo e comprovado de lesão ao bem jurídico. A punição de uma agressão em sua fase ainda embrionária, embora aparentemente útil do ponto de vista da defesa social, representa ameaça à proteção do indivíduo contra uma atuação demasiadamente intervencionista do Estado.

Por esse ângulo, é imperativo enquadrar as notícias falsas como crimes de perigo concreto, uma vez que, sua veiculação e disseminação através das mídias digitais podem acarretar danos à sociedade, levando-os a cometer ações de maneira incorreta, criando, dessa forma, o perigo concreto (Capez, 2019).

À vista disso, nota-se que a intenção de criar e disseminar desinformação enquadra-se cabalmente no âmbito penal, uma vez que os danos causados por essa conduta afetam diretamente a sociedade, ocasionando problemas para várias pessoas que, por falta de instrução, acabam por acreditar nas informações veiculadas nas redes.

Conquanto a falta de tipificação da conduta de produção e compartilhamento de notícias fraudulentas por meio da internet no sistema jurídico penal brasileiro, nota-se que sua prática pode servir de meio para infringir bens jurídicos já resguardados pelo Direito Criminal, assim como, produzir e compartilhar notícias falsas na internet com uso de *deepfake*, conforme será exibido a seguir.

3.3.1 Lei Carolina Dieckmann (Lei nº 12.737/2012)

É evidente que a internet está em constante evolução, e é crucial que a legislação brasileira acompanhe esse dinamismo para assegurar a proteção dos direitos constitucionais em consonância com o progresso tecnológico. Conforme dito no capítulo anterior, no mês de maio de 2012, a atriz Carolina Dieckmann enfrentou um momento doloroso quando foi vítima de ataques de hackers. Esses indivíduos invadiram o e-mail da atriz, realizaram o download

de 36 fotos e conversas íntimas e a ameaçaram exigindo o pagamento de R$10 mil para evitar a divulgação das imagens. Carolina optou por não ceder à chantagem, porém, suas fotos foram divulgadas na internet sem sua autorização.

Esse incidente ganhou destaque nacional e foi um dos motivos que levaram à criação da Lei n° 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann. A legislação foi sancionada em novembro do mesmo ano pela então presidente, Dilma Rousseff. Essa lei teve como objetivo tipificar os crimes informáticos, preenchendo uma lacuna anteriormente existente. Conforme estabelecido no Artigo 1º, a Lei trata da tipificação criminal de delitos informáticos e estabelece outras medidas correlatas (Brasil, 2012).

A abrangência da lei vai além da cobertura dos delitos de divulgação de fotos e imagens, estendendo-se a uma série sequencial de crimes informáticos. Ela também prevê o aumento da pena quando o crime for cometido contra autoridades como o Presidente da República, membros do Supremo Tribunal Federal, prefeitos, governadores e demais autoridades do poder executivo e legislativo (Brasil, 2012).

Dentre os delitos contemplados, está a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança, com o propósito de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo, ou ainda instalar vulnerabilidades visando à obtenção de vantagem ilícita (Brasil, 2012).

3.3.2 Crimes decorrentes do uso e disseminação de Notícias Falsas com emprego de *deepfake* pela Internet

O meio virtual se tornou um ambiente propício para a produção e proliferação de notícias falsas, haja vista a possibilidade de compartilhamento através das redes sociais e aplicativos de mensagens instantâneas, principalmente com advento das inteligências artificiais. Malgrado a criação e disseminação de *fake news* por meio da internet, inclusive com o uso de *deepfake*, não constituírem, por si só, crime no nosso ordenamento jurídico-penal pátrio, não significa que tais ações não sejam capazes de resultar crime de internet, conforme será explicado a seguir.

Inobstante isso, para haver condenação penal é imperativo a presença de lesividade comprovada da conduta, em outras palavras, é preciso que a conduta do agente seja considerada lesiva ao indivíduo ou sociedade, caso não haja tal premissa, inexiste motivação para a intervenção do direito penal e, consequentemente, resultar na imposição de uma

potencial pena de prisão ao responsável. No que concerne ao princípio da lesividade, Luigi Ferrajoli (2002, p. 374) preleciona que:

> O princípio da lesividade impõe à ciência e à prática jurídica precisamente o ônus de tal demonstração. A necessária lesividade do resultado, qualquer que seja a concepção que dela tenhamos, condiciona toda justificação utilitarista do direito penal como instrumento de tutela e constitui seu principal limite axiológico externo. Palavras como "lesão", "dano" e "bem jurídico" são claramente valorativas. Dizer que um determinado objeto ou interesse é um "bem jurídico" e que sua lesão é um "dano" é o mesmo que formular um juízo de valor sobre ele; e dizer que é um "bem penal" significa, ademais, manifestar um juízo de valor que avaliza a justificação de sua tutela, recorrendo a um instrumento extremo: a penal.

Com base nesse princípio, observa-se que a condenação criminal requer a comprovação da lesividade do ato, ou seja, a ação realizada deve ser considerada prejudicial ao indivíduo ou à coletividade. Sem esse aspecto, não há justificativa para a intervenção do direito penal, não sendo razoável impor uma possível pena de prisão ao agente.

3.3.2.1 Crimes contra a honra

Os crimes contra a honra, como a calúnia, a difamação e a injúria, encontram-se previstos do art. 138 até o art. 145 do Código Penal Brasileiro. Esses tipos penais representam práticas que podem ser cometidas por meio da produção e compartilhamento de notícias falsas pela internet, sobretudo, com o auxílio do *deepfake*.

Certamente, a calúnia encontra tipificação no artigo 138 do Código Penal. De acordo com a interpretação do texto legal, a calúnia acontece quando alguém atribui falsamente a outra pessoa a prática de um fato considerado crime, sendo passível de punição com detenção de seis meses a dois anos, além de multa. Como citado por Furlaneto Neto, Santos e Gimenes (2018, p. 56):

> Caluniar, de acordo com o art. 138 do Código Penal pátrio, significa acusar falsamente alguém da prática de fato definido como crime, colocando em dúvida a sua credibilidade no meio social, atingindo, de tal forma, sua honra objetiva, isto é, o conceito externo que os outros têm da pessoa caluniada.

Em conformidade com o entendimento supra-expendido, entende-se que o art. 138, do Código Penal busca proteger a honra objetiva, que se refere à reputação ou à imagem de uma pessoa diante de terceiros. Além disso, há a possibilidade de responsabilização penal àquele que, mesmo sabendo que a imputação é falsa, propala ou divulga, conforme §1°, do art. 138, do Código Penal. Tal direito à reputação também é assegurado aos mortos, de acordo com previsão legal contida no §2°, do referido artigo de Lei.

No que se refere ao sujeito ativo do crime de calúnia, pode ser qualquer indivíduo. Da mesma forma, em relação ao sujeito passivo, este pode ser qualquer pessoa, incluindo pessoas

jurídicas, desde que a imputação esteja relacionada à prática de crime ambiental (Nucci, 2020).

O elemento subjetivo no crime calúnia "é a vontade específica de macular a imagem de alguém (*animus diffamandi*)", sucedendo a execução do crime "no momento em que a imputação falsa chega ao conhecimento de terceiros, independentemente de resultado naturalístico" (Nucci, 2020, p. 136).

O §3° do art. 138 do Código Penal prevê a exceção da verdade, um mecanismo processual que representa uma forma de defesa indireta. Tal dispositivo permite que o acusado de calúnia prove a veracidade da acusação do crime imputado. Se a veracidade do crime imputado for comprovada, e, portanto, não sendo uma imputação falsa como exigido pelo tipo penal do artigo 138, o crime de calúnia não seria configurado.

Não obstante, existem três situações que a exceção da verdade é vedada no direito penal brasileiro, quais sejam: (1) quando "o fato imputado à vítima constitua crime de ação privada e não houve condenação definitiva sobre o assunto (§3º, I)"; (2) "quando a calúnia envolver o Presidente da República ou chefe de governo estrangeiro (§3.º, II)", ou ainda, (3) "quando o assunto já foi debatido e julgado, em definitivo, pelo Poder Judiciário, tendo havido absolvição do ofendido (§3.º, III)" (Nucci, 2020, p. 456).

Seguidamente, o Código Penal estabelece a difamação como um tipo penal incriminador, descrito no artigo 139. Conforme a norma legal, constitui-se crime de difamação a imputar a alguém de fato que seja ofensivo à sua reputação. Tal prática pode ser punida com pena de detenção de três meses a um ano, cumulada com multa. Ao abordar os elementos objetivos do tipo, Guilherme Nucci (2020, p. 460) dispõe que:

> Difamar significa desacreditar publicamente uma pessoa, maculando-lhe a reputação. Nesse caso, mais uma vez, o tipo penal foi propositadamente repetitivo. Difamar já significa imputar algo desairoso a outrem, embora a descrição abstrata feita pelo legislador tenha deixado claro que, no contexto do crime do art. 139, não se trata de qualquer fato inconveniente ou negativo, mas sim de fato ofensivo à sua reputação. Com isso, excluiu os fatos definidos como crime – que ficaram para o tipo penal da calúnia – bem como afastou qualquer vinculação à falsidade ou veracidade dos mesmos. Assim, difamar uma pessoa implica divulgar fatos infamantes à sua honra objetiva, sejam eles verdadeiros ou falsos. A pena é de detenção, de três meses a um ano, e multa.

Nesse tipo penal, o bem jurídico protegido é a honra objetiva, que compreende a reputação ou a imagem de uma pessoa perante terceiros. O sujeito ativo desse crime pode ser qualquer indivíduo, da mesma forma que o sujeito passivo, incluindo pessoas jurídicas, já que estas também têm uma imagem a preservar e podem ser afetadas por ações difamatórias. No tocante ao elemento subjetivo do tipo "é a vontade específica de macular a imagem de alguém

(*animus diffamandi*)", ocorrendo a execução do crime "no momento em que a imputação chega ao conhecimento de terceiros, independentemente do resultado naturalístico" (Nucci, 2020).

De acordo com o parágrafo único do artigo 139 do Código Penal, a difamação também contempla a possibilidade da exceção da verdade. No entanto, essa exceção está limitada às situações em que o ofendido é um funcionário público, e a ofensa se refere ao desempenho de suas funções.

Assim, na prática do crime de difamação permite-se exceção à verdade por conta do interesse estatal, situação em que é necessário investigar a veracidade do conteúdo difamatório e, dependendo do caso, aplicar as sanções apropriadas ao servidor envolvido.

Em sequência, o delito de injúria, descrito no art. 140 do Código Penal, que consiste em ofender a dignidade ou o decoro de alguém, acarreta uma pena de detenção de um a seis meses, ou multa.

No que diz respeito ao sujeito ativo do crime de injúria, igualmente a calúnia e difamação, poderá ser qualquer indivíduo, enquanto o sujeito passivo poderá ser apenas pessoa natural, haja vista a ausência de subjetividade da honra relativa a pessoa jurídica. Ademais, tratando-se de ofendido inimputável, é necessário a análise concreta do caso para que seja vista a capacidade de ocupar o polo passivo do crime de injúria, considerando que, em algumas situações, os inimputáveis podem não ter dissentimento sobre dignidade e decoro.

Tal situação ocorre pelo fato de que o bem jurídico tutelado pelo Direito Penal no crime de injúria diz respeito à honra subjetiva do sujeito, ou seja, a sua visão sobre si mesmo. Ao tratar sobre os elementos objetivos desse tipo penal, Guilherme Nucci (2020, p. 675) disserta que:

> Injuriar significa ofender ou insultar (vulgarmente, xingar). No caso presente, isso não basta. É preciso que a ofensa atinja a dignidade (respeitabilidade ou amor-próprio) ou o decoro (correção moral ou compostura) de alguém. Portanto, é um insulto que macula a honra subjetiva, arranhando o conceito que a vítima faz de si mesma. A pena é de detenção, de um a seis meses, ou multa. Conferir o capítulo XIII, item 2.1, da Parte Geral. Embora, a maneira mais comum de se praticar a injúria seja por meio de xingamentos verbais, são admitidas várias outras formas, inclusive por gestos, comportamentos ou até mesmo por omissão. Conforme o cenário, a recusa a um cumprimento pode figurar uma injúria, conduta que se dá na forma omissiva. Por outro lado, utilizar vestimenta inadequada em lugar de respeito também é conduta apta a construir a injúria. Na verdade, todas as atitudes tendentes a ferir a dignidade alheia constituem elementos válidos para a realização do crime. Para analisar os vários comportamentos humanos, no contexto da injúria, depende-se da adequação social, 'restringindo-se o tipo do delito de injúria àqueles casos que excedam em muito o tolerável socialmente em cada momento histórico'.

Ante esses aspectos, observa-se que o elemento subjetivo do crime de injúria é "vontade específica de magoar e ferir a autoimagem de alguém (*animus injuriandi*)", visto que o cometimento "ocorre no momento em que a imputação chega ao conhecimento do ofendido, independentemente de resultado naturalístico e da ciência de terceiros" (Nucci, 2020, p. 465).

De mais a mais, cumpre ressaltar que, em se tratando de injúria cometida por meio da raça, cor, etnia, religião ou a condição de pessoa idosa ou portadora de deficiência, a pena imposta deverá representar de um a três anos e multa, de acordo com o previsto §3°, do art. 140, do Código Penal.

De acordo com o artigo 141 do Código Penal, as penas por calúnia, difamação e injúria são aumentadas em um terço quando cometidas contra certas autoridades ou em certas circunstâncias específicas. Isso inclui o Presidente da República ou chefes de governo estrangeiros (art. 141, inciso I); funcionários públicos devido às suas funções, assim como o Presidente do Senado Federal, da Câmara dos Deputados ou do Supremo Tribunal Federal (art. 141, inciso II). Também quando ocorrem na presença de várias pessoas ou por meios que facilitem a divulgação (art. 141, inciso III). Há, além disso, um agravante quando os crimes são cometidos contra crianças, adolescentes, pessoas acima de 60 anos ou pessoas com deficiência, exceto nos casos em que o ofensor comprovar a exceção da verdade, quando essa é admitida.

Conforme o artigo 141 do Código Penal, se os crimes de calúnia, difamação e injúria forem cometidos mediante pagamento ou promessa de recompensa, a pena é dobrada (art. 141, §1°). Além disso, se esses crimes forem cometidos ou divulgados em quaisquer modalidades das redes sociais da internet, a pena é triplicada.

De acordo com Furlaneto Neto, Santos e Gimenes (2018, p. 53), a tipificação dos crimes contra a honra praticados por meio da internet não demandaria uma alteração legislativa, uma vez que o artigo 141, inciso III, do Código Penal já prevê o aumento de pena nos casos em que o crime for cometido por um meio que facilite a sua divulgação. No entanto, após a publicação da obra dos autores, foi introduzido o § 2° no artigo 141 do Código Penal, estabelecendo expressamente a aplicação em triplo da pena nos casos em que os crimes contra a honra são cometidos ou divulgados em qualquer modalidade das redes sociais da internet.

Os delitos mencionados podem ser facilmente perpetrados por meio da criação e difusão de notícias falsas pela internet. Seguindo a classificação de Jesus e Milagre (2016), esses crimes seriam considerados crimes informáticos impróprios, uma vez que utilizam a

tecnologia da informação (englobando a internet em geral, redes sociais, aplicativos de mensagens instantâneas e similares) como meio para atacar bens jurídicos já resguardados pelo Direito Penal.

Em consonância com a pesquisa realizada no site do Superior Tribunal de Justiça, verifica-se a reafirmação do combate à produção e compartilhamento de notícias falsas pela internet, visando a proteção dos bens jurídicos relacionados à honra objetiva e subjetiva. Esse entendimento foi corroborado na decisão de denegação do habeas corpus n° 587235 - PA17. Em síntese, o caso envolveu suspeitos que se associaram para cometer os crimes de difamação, injúria e calúnia. Segundo a decisão monocrática proferida pelo Relator, Ministro Olindo Menezes (Desembargador Convocado do TRF da 1ª Região), os suspeitos teriam criado páginas na internet que interagiam entre si, compartilhando conteúdos com o intuito de difamar a vítima. Essas páginas veiculavam informações que buscavam manchar a imagem pública da vítima, atribuindo-lhe condutas desonrosas e alegando envolvimento em atividades criminosas.

Portanto, em face das características dos crimes acima referenciados, percebe-se que a criação e a disseminação de notícias falsas na internet, sobretudo com o emprego de *deepfake*, embora, intrinsecamente, não constitua crime na ordem jurídico-penal brasileira, poderá configurar um crime impróprio de internet e lesar bens jurídicos já protegidos pelo Direito Penal nacional, como é o caso dos crimes contra a honra, tais como calúnia, difamação e injúria.

3.4 A INTERVENÇÃO DO DIREITO PENAL NA RESPONSABILIZAÇÃO PELA PRODUÇÃO E COMPARTILHAMENTO DAS FAKES NEWS

A responsabilidade penal refere-se à obrigação legal de enfrentar as consequências de uma ação criminosa. Em resumo, quando alguém que pode ser responsabilizado por seus atos comete um crime, essa pessoa está sujeita a punições, aplicadas por meio de penas que podem envolver restrição da liberdade, restrição de direitos ou pagamento de multa.

Nesse contexto, é imperativo avaliar se, ao compartilhar informações falsas, a pessoa agiu intencionalmente ou não, isto é, se houve dolo (intenção) ou culpa (negligência). Nesse sentido, a análise recai sobre o crime doloso, conforme delineado no artigo 18, inciso I do Código Penal, o qual define o dolo como a situação em que o agente deseja o resultado do seu ato ou assume o risco de produzi-lo. Em relação ao conceito de dolo, Cleber Masson (2019, on-line) aborda que:

> O dolo, no sistema finalista, integra a conduta, e, consequentemente, o fato típico. Cuida-se do elemento psicológico do tipo penal, implícito e inerente a todo crime doloso. Dentro de uma concepção causal, por outro lado, o dolo funciona como elemento da culpabilidade. Em consonância com a orientação finalista, por nós adotado, o dolo consiste na vontade e consciência de realizar os elementos do tipo incriminador.

Assim, depreende-se que ao aplicar o conceito de dolo no ato de compartilhar notícias falsas com o emprego de *deepfake*, há a possibilidade de ficar sujeito a pena prevista, a partir do momento em que tiver comprovado a vontade consciente do agente em atingir o resultado.

Outrossim, o crime culposo, conforme estabelecido no Artigo 18, inciso II do Código Penal, ocorre quando o agente provoca o resultado por imprudência, negligência ou imperícia. Além disso, o Parágrafo Único desse mesmo artigo estipula que, exceto nos casos expressos em lei, ninguém pode ser penalizado por um ato considerado crime, a menos que o cometa de forma intencional (dolosa).

Luiz Regis Prado (2020) diferencia o crime culposo do doloso: no culposo, critérios normativos atribuem significado à conduta; no doloso, a análise do dolo é essencial. Essa distinção é mais notável na tipicidade: no culposo, há ação de risco proibido; no doloso, o resultado é fruto de uma ação específica.

No caso em questão, implica-se que não há possibilidade de divulgação ou criação culposa de fake news (e *deepfake*), pois tal ato depende estritamente da vontade do agente, ou seja, o indivíduo detém total controle sobre tais atos, e pode muito bem presumir o quão maléfico podem ser as suas atitudes.

Os crimes contra a honra, tais como calúnia, difamação e injúria, possuem como requisito essencial à configuração do dolo, ou seja, a intenção consciente do agente de difamar, caluniar ou injuriar alguém (Brasil, 1940).

No âmbito do Direito Penal Brasileiro, a caracterização de um crime como culposo somente ocorre quando expressamente previsto na legislação. A ausência dessa previsão específica nos tipos de crime relacionados à ofensa à honra restringe a imputação desses delitos à modalidade dolosa, isto é, àquela que requer a comprovação da intenção consciente do agente para sua configuração (Pereira, 2020).

Considerando que a disseminação de fake news pode ser enquadrada como crimes contra a honra, é observado que esses delitos não admitem a modalidade culposa, sendo estritamente limitados à forma dolosa, ou seja, à intenção consciente do agente de difamar, caluniar ou injuriar alguém.

Com o intuito de garantir a intervenção do Poder Público de maneira imediata, é desejável conciliar a preservação da liberdade individual, considerada um valor supremo, com a proteção da dignidade da pessoa humana, tudo isso em conformidade com as exigências do Estado Democrático de Direito (Nucci, 2020).

A Constituição Federal de 1988, ao determinar as modalidades de penas que devem ser adotadas pela legislação ordinária, implícita e naturalmente consagra o princípio da proporcionalidade, o qual é um corolário da aplicação da justiça, que visa a conceder a cada um, o que é devido, conforme seu merecimento. No artigo 5º, XLVI, são estabelecidas as seguintes penalidades: a) privação ou restrição da liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos.

Diante disso, o poder judiciário reconhece a falta de controle sobre o conteúdo postado e compartilhado nas redes sociais. No entanto, há a compreensão de que não se deve recorrer ao direito penal para todos os casos de possíveis fake news, pois isso poderia resultar em um acúmulo excessivo de processos que, eventualmente, não teriam desfecho conclusivo.

É fundamental considerar que todo indivíduo pode ser responsabilizado pelas ações que pratica, especialmente quando tais atos afetam as relações sociais de outras pessoas. Atualmente, inúmeros temas circulam nas redes sociais e são compartilhados pelos usuários, o que pode resultar em diversas consequências, especialmente quando se trata de fake news. Essas informações falsas podem desencadear uma série de problemas, incluindo impactos psicológicos nas vítimas, desde situações simples, como se isolar e parar de interagir com amigos, até casos mais graves, como o suicídio (Cerdeira, 2020).

Portanto, é essencial realizar uma análise no caso específico para determinar se o responsável pela propagação das notícias falsas pretendia ou ao menos poderia prever os efeitos prejudiciais e a extensão de suas ações.

A questão de tipificação das fake new*s* nos coloca no olho do furação do fervoroso debate entre eficácia penal e garantia individual, no qual o legislador deve friamente sopesar os alcances do tipo penal incriminador, para que possa com a sua existência defender bens jurídicos relevantes, e ao mesmo tempo resguardar garantias individuais, fazendo com que garantias não sejam usadas como escudo por delinquentes, e que a eficiência do tipo penal seja alcançada com a punição daqueles que realmente ultrapassando seus direitos violem bens jurídicos individuais ou coletivos, mas que nunca seja utilizada como meio de promoção de censura, sendo este verdadeiro dilema que requer toda nossa atenção.

Ainda, em conformidade com o princípio da proporcionalidade, também denominado princípio da razoabilidade ou da conveniência das liberdades públicas, a definição de tipos

penais incriminadores deve oferecer benefícios à sociedade, já que impõe um ônus a todos os cidadãos por meio da ameaça de punição (Masson, 2019).

A responsabilização criminal do agente que produz ou dissemina fake news se torna evidente, mesmo na ausência de uma lei específica sobre o assunto. Nesses casos, o magistrado deve aplicar as normas existentes que melhor se adequem a cada situação específica, a fim de assegurar a proteção do bem jurídico tutelado pelo Estado.

CONSIDERAÇÕES FINAIS

Notadamente, a internet representa nos dias atuais a principal ferramenta utilizada pelos indivíduos em sociedade para o desenvolvimento de suas relações sociais, provocando mudanças estruturais que trazem consigo novos desafios para a sociedade moderna e para as ciências jurídicas. Dentre os desafios que emergem com o avanço tecnológico, encontram-se as *deepfakes,* inteligência artificial que propicia a manipulação de fotos, vídeos e áudios, criando uma falsa percepção da realidade e, as *fakes new*s, que compreendem as notícias fabricadas com a intenção de ludibriar e manipular as massas populacionais.

Nesse contexto, o presente trabalho obteve como parâmetro identificar a possibilidade de responsabilização dos indivíduos que produzem e compartilham notícias fraudulentas, com o emprego de *deepfake,* no ciberespaço, para justificar a necessidade de entender os efeitos da manipulação de mídia tanto esfera criminal quanto na cível, com a finalidade de promover subsídios para o desenvolvimento de mecanismos legais e regulatórios capazes de combater tal prática de forma eficaz, além de preservar a integridade da informação e do tecido social, a partir de uma revisão bibliográfica, que abrangeu a consulta a livros, revistas e periódicos pertinentes ao tema em referência, bem como recorreu-se a literatura jurídico-científica pertinente. Para compreender a análise sobre como a utilização de *deepfake,* como manipulação de mídia, se configura como uma ferramenta poderosa para a disseminação de desinformação, considerando o papel dos instrumentos jurídicos pertinentes para combater esse fenômeno e suas potenciais consequências, estabelecer-se-á três objetivos específicos.

Primeiramente, observou-se que as notícias falsas não são um fenômeno recente, mas ganharam mais notoriedade no cenário atual devido a facilidade de compartilhamento por meio das redes sociais e veículos de informação, além do auxílio da inteligência artificial que torna as notícias falsas mais convincentes, como é o caso da *deepfake.* Em seguida, a análise permitiu observar que a legislação em vigor, sozinha, não é suficiente para combater o fenômeno das *fakes news*, principalmente com a utilização de *deepfake,* uma vez que não há a possibilidade de responsabilização direta, ainda que na esfera cível, dos responsáveis pela produção e compartilhamento do conteúdo fabricado. Outrossim, identifica-se que as notícias falsas causam danos imensuráveis aos indivíduos e confrontam-se continuamente com princípios constitucionais presentes no Estado Democrático de Direito. Essa constatação, revela a necessidade premente de uma regulamentação mais severa, uma vez que o Marco Civil da Internet estabelece apenas diretrizes gerais sobre a utilização da internet no país.

Outrossim, diante da necessidade de elaboração de novas medidas legislativas para ajudar a combater disseminação de *deepfake* e fake news, surge o Projeto de Lei nº 2.630/2020, como um instrumento crucial para regulamentar o uso de plataformas on-line no que diz respeito à produção e disseminação de notícias falsas. Por último, a pesquisa possibilitou concluir que, apesar da inexistência de um tipo penal específico que incrimine aqueles que produzem e compartilham fake news pela internet, tal conduta pode ser enquadrada como meio para a prática de crimes crimes mediatos/indiretos, como os crimes contra a honra objetiva e subjetiva tipificados no Código Penal a partir do art. 138, a saber: calúnia, difamação e injúria.

Em conclusão, nota-se a possibilidade de responsabilização dentro do ordenamento jurídico brasileiro, uma vez que as fake news, juntamente com as *deepfakes*, ao servirem como método para a prática de diversos crimes na internet, não apenas violam os direitos fundamentais, mas também prejudicam outros direitos essenciais à sociedade. Esses direitos incluem a honra objetiva e subjetiva, a privacidade e a administração da justiça. Contudo, apesar da utilidade na criação de meios específicos para combater a disseminação de fake news e *deepfake*, permanece o questionamento se o atual ordenamento jurídico dispõe de mecanismos suficientes para contê-la. É essencial que o Poder Legislativo e Judiciário atuem de maneira decisiva nos conflitos relacionados a esse tema, pois a falta de ação pode criar a percepção na sociedade de que não existem normas eficazes para combater a propagação de desinformação, comprometendo a eficácia das medidas preventivas estabelecidas.

REFERÊNCIAS

ALLCOTT, M. G. H. **Social media and *fake news* in the 2016 election. Journal of Economic Perspectives**. 2017. Disponível em: https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211. Acesso em: 23 ago. 2023.

ALMEIDA, C. B. M. V. **Ataque à imagem de Marielle Franco revela a lógica das *Fake news*.** 2018. Revista Subjetiva.

ARAS, Vladimir. **Breves Comentários ao Marco Civil da Internet.** Disponível em: http://blogdovladimir.wordpress.com./2014/05/05/breves-comentarios-ao-marco-civil-da-internet. Acesso em: 30 set. 2023.

ASSIS, L. B. de. (2020). **Direito à informação verdadeira em tempos de *fake news*.** Conteúdo Jurídico. https://conteudojuridico.com.br/consulta/Artigos/54433/direito-informao-verdica-em-tempos-de-fake-news. Acesso em: 01 de out. 2023

BARROS, Laura; OLIVEIRA, Gustavo. *Fake news*, **liberdade de expressão e moderação nas redes sociais: tendências.** Disponível em: https://www.conjur.com.br/2021-out-17/publicopragmatico-fake-news-liberdade-expressao-moderacao-redes-sociais-tendencias. Acesso em: 20 out. 2023.

BASTOS, Celso Ribeiro. Martins, Ives Gandra. **Comentários à Constituição do Brasil: promulgada em 5 de outubro de 1988.** Imprenta: São Paulo, Saraiva, 2004.

BBC. Disponível em: https://www.bbc.com/portuguese/internacional-41843695. Acesso em: 05 de jul. de 2023.

BILNEY, L. About Liz Bilney. 2016. **Leave.EU on-line.** Disponível em: https://www.bbc.com/news/uk-politics-44080096. Acesso em: 19 ago. 2023.

BINICHESKI, P. R. (2021, 9 de junho). **Garantias do consumidor e liberdade de expressão na internet: o dilema das redes sociais**. Consultor Jurídico. https://www.conjur.com.br/2021-jun-09/garantias-consumo-liberdade-expressao-internet-dilema-redes-sociais. Acesso em: 01 de out. 2023.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral (arts. 1º a 120**). 26. ed. São Paulo: Saraiva Educação, 2020. 1 v. p. 57.

BLOCH, Marc. **Réflexions d'un historien sur les fausses nouvelles de la guerre.** 3. ed. Paris: Éditions Allia, 2012. Disponível em: https://hal.science/hal-03325572/file/bloch-marc.pdf. Acesso em: 03 out. 2023.

BOBBIO, Norberto. **A era dos direitos. Tradução de Carlos Nelson Coutinho.** Rio de Janeiro: Elsevier, 2004. p. 13.

BOULOS, G. [@GuilhermeBoulos]. (2022, 15 de setembro). **Conteúdo do tweet. Twitter.** https://twitter.com/GuilhermeBoulos/status/1560315298821062656?s=20. Acesso em: 03 de out. 2023.

BRAGA, Renê Morais da Costa. **A indústria das *fake news* e o discurso de ódio.** In: PEREIRA, Rodolfo Viana (Org.). **Direitos políticos, liberdade de expressão e discurso de ódio. Volume I.** Belo Horizonte: IDDE, 2018. p. 203-220. Disponível em:

http://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/4443/2018_pereira_direitos_politicos_liberdade.pdf?sequence=1#page=205. Acesso em: 10 jun. 2023.

BRANCO, Sérgio, ***Fake news* e o caminho para fora da bolha. Interesse Nacional.** Ago-Out. 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/08/sergio-fakenews.pd.Acesso em: 05 out. 2023.

FATO. **Nova *fake news* sugere que ivermectina é 90% eficaz na prevenção à covid-19, 2021.** Disponível em: https://www.brasildefato.com.br/2021/03/12/nova-fake-news-sugere-que-ivermectina-e-90-eficaz-na-prevencao-a-covid-19. Acesso em: 30 ago. 2023.

BRASIL Superior Tribunal de Justiça. **Recurso Especial nº 1.642.997/RJ. Recorrente: Facebook Serviços Online do Brasil LTDA. Recorrido: Fernando Cândido da Costa. Relatora Min. Nancy Andrighi.** Publicado em 15 Set 2017. Disponível em: http://www.stj.jus.br/sites/portalp/Inicio. Acesso em: 03 e out. 2023.

BRASIL, Jusbrasil. **O que é uma Constituição?.** Jusbrasil, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/887832733/o-que-e-uma-constituicao. Acesso em: 29 de set. de 2023.

BRASIL. **Câmara dos Deputados. Projeto de Lei nº 2.630/2020. Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334. Acesso em: 10 out. 2023.

BRASIL. **Comissão dos Direitos Humanos da Ordem dos Advogados. Direitos Humanos: Cidadania e Igualdade.** 1a Ed. São João do Estoril: Princípia Editora, 2006.

BRASIL. Lei n. 12.737/12. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Extraído de: http://www.planalto.gov.br/ccivil_03/ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 nov. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).**

BRASIL**. Supremo Tribunal Federal (STF).** Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=14588363. Acesso em: 04 e out. 2023.

BUNK, J.; BAPPY, J.; MOHAMMED, T.; NATARAJ, L.; FLENNER, A.; MANJUNATH, B.; CHANDRASEKARAN, S.; PETERSON, L**. Detection and localization of image forgeries using resampling features and deep learning.** 2017. Recuperado de https://arxiv.org/abs/1707.00433. Acesso 03 mar. 2023.

BUSSULAR, Luis Filipe. **O impacto das *Fake news* na vida em sociedade.** Disponível em: https://lfbussular.jusbrasil.com.br/artigos/577903609/o-impacto-dasfake-news-na-vida-emsociedade?ref=topic_feed. Acesso em: 11 de jul. 2023.

CABRAL, Isabela. **O que é deepfake? Inteligência artificial é usada pra fazer vídeo falso.** TechTudo. Disponível em:

https://www.techtudo.com.br/noticias/2018/07/o-que-e-deepfake-inteligencia-artificial-e-usada-pra-fazer-videosfalsos.ghtml. Acesso em: 22 mai. 2023.

CANOTILHO, José Joaquim; MOREIRA, Vital. **Constituição da República Portuguesa: anotada.** Coimbra: Coimbra Editora, 2014.

CAPEZ, Fernando**. Curso de direito penal parte geral: arts. 1º a 120. 23.** ed. São Paulo: Saraiva Educação, 2019. 1v.

CARDOSO, P. M. (2023). **Entenda de uma vez por todas o conceito de neutralidade da rede.** Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/1839681291/entenda-de-uma-vez-por-todas-o-conceito-de-neutralidade-da-rede. Acesso em: 04 de out. 2023.

Caruso, Tiago. (2021). **"Deve o direito penal proibir a difusão das *Fake news*.**" Recuperado de https://www.ibccrim.org.br/noticias/exibir/8545. Acesso em: 04 nov. 2023.

CARVALHO, Antonia Rafaela Fernandes. **Twitter e facebook: liberdade de expressão e vida privada. Revista Direito e Liberdade.** Natal. 2013. Disponível em: https://core.ac.uk/download/pdf/16047038.pdf. Acesso em: 16 set. 2023.

CEPIK, Marco. **Direito à Informação: Situação Legal e Desafios.** Revista IP - Informática Pública, Belo Horizonte, v. 02, n. 02, p. 43-56, dez. 2000.

CHESNEY, Robert. **CITRON, Danielle. Deepfakes and the New Disinformation War. 2019.** Disponível em: https://scholarship.law.bu.edu/shorter_works/76. Acesso 12 mai. 2023.

CHOI, Y. et al. **StarGAN: Unified Generative Adversarial Networks for MultiDomain Image-to-Image Translation.** 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City.

CINTRA, H. J. M. **Dimensões da interatividade no mundo digital.** Disponível em: http://www.terraforum.com.br/biblioteca/Documents/libdoc00000032v001Dimensoes%20da%20Interatividade%20na%20Cultura%20Dig.pdf. Acesso em: 08 set. 2023.

COELHO, Leonardo. **Lei das *Fake news.* Politize, julho de 2020.** Disponível em: https://www.politize.com.br/lei-das-fake-news. Acesso em: 22 out. 2023.

COLOMBO, Cristiano; NETO FACCHINI, Eugênio. **Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça.** Revista Brasileira de Políticas Públicas, Brasília, volume 7, 2017, n° 3, p. 2018.

CONJUR. **Aprovado pelo Senado, PL das Fake news é ampliado na Câmara.** Disponível em: https://www.conjur.com.br/2021-nov-05/aprovado-senado-pl-fake-news-ampliado-camara. Acesso em: 6 nov. 2023.

CORMEN, Thomas H, **Algoritmos: teoria e prática.** 3. ed. Rio de Janeiro: Campus, 2012.

DANG, H. et al. **On the Detection of Digital Face Manipulation**, Outubro 2019.

DANTAS, T. "Web 2.0"; **Brasil Escola.** Disponível: http://brasilescola.uol.com.br/informatica/web-20.htm. Acesso em: 09 set. 2023.

DARNTON, Robert**. The true history of fake news. The New York review of books.** Disponível em; https://www.nybooks.com/online/2017/02/13/the-true-history-of-fake-news. Acesso em: 02 ago. 2023.

DINIZ, Irlla. **Os usos da mídia em aulas de Educação Física Escolar: possibilidades e dificuldades.** In: Revista Movimento. Porto Alegre, v. 18, n. 03. 2012.

DOMINGOS, Roney. **É #FAKE foto que mostra a rainha Elizabeth II dando título de cavaleiro a um gato.** 2022. Disponível em: https://g1.globo.com/fato-ou-fake/noticia/2022/04/27/e-fake-foto-que-mostra-rainha-elizabeth-ii-dando-titulo-de-cavaleiro-a-um-gato.ghtml. Acesso em: 29 ago. 2023.

EDUVIRGES, J. R.; SANTOS, M. N. **A contextualização da Internet na sociedade da informação. 2013.**

FACEAPP. **FaceApp, 2017.** Disponível em: https://www.faceapp.com. Acesso em: 10 Jul. 2023.

FARIAS, Cristiano Chaves; ROSENVALD, Nelson; NETTO, Felipe Peixoto Braga. **Curso de Direito Civil: responsabilidade civil.** 4. ed. Salvador: JusPodivm, 2017.

FARIAS, Edilson Pereira de. **Liberdade de expressão e comunicação.** São Paulo: Revista dos Tribunais, 2004.

FERNANDES, Alexandre Cortez. Direito Civil: **Responsabilidade Civil.** Caxias do Sul, RS: Educs, 2013; p. 167.

FERRAJOLI, Luigi. Direito e Razão: **Teoria do garantismo penal.** – São Paulo: RT, 2002. p. 374.

FILHO, Sérgio Cavalieri. **Programa de responsabilidade civil.** 10. ed. São Paulo: Atlas, 2012.

FOTOS PESSOAIS DA ATRIZ CAROLINA DIECKMANN VAZAM NA INTERNET. G1. s/d, 05/05/2012. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2012/05/fotos-pessoais-da-atriz-carolina-dieckmann-vazam-na-internet.html. Acesso em: 02 de out. 2023.

FURLANETO NETO, Mario; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico.** 2. ed. São Paulo: Edipro, 2018. 238 p.

G1. (2022, 19 de setembro). **Deepfake: conteúdo do Jornal Nacional é adulterado para desinformar os eleitores.** G1. https://g1.globo.com/jornal-nacional/noticia/2022/09/19/deepfake-conteudo-do-jornal-nacional-e-adulterado-para-desinformar-os-eleitores.ghtml. Acesso em: 03 de out. de 2023.

GABRIEL, Martha. **Marketing na era digital: conceitos, plataformas e estratégias.** São Paulo: Novatec, 2010.

GOMES, Cesar Augusto. **Os 7 tipos de *Fake news* sobre a Covid-19. 2020.** Disponível em: https://www.blogs.unicamp.br/covid-19/os-7-tipos-de-fake-news-sobre-a-covid-19. Acesso em: 27 ago. 2023.

BRASIL. (2018, novembro). **Artigo 19º: Todo ser humano tem direito à liberdade de expressão e opinião. Ministério da Mulher, da Família e dos Direitos Humanos**. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2018/novembro/artigo-19deg-todo-ser-humano-tem-direito-a-liberdade-de-expressao-e-opiniao-1. Acesso em: 01 out. 2023.

GÜERA, D., DELP, E. J. (2018). **Deepfake video detection using recurrent neural networks. In IEEE International Conference on Advanced Video and Signal-based Surveillance (to appear).**

GUERRA FILHO, Willis Santiago. CARNIO, Henrique Garbellini. **Metodologia Jurídica Político Constitucional e o Marco Civil da Internet: Contribuição ao Direito Digital. In. Marco Civil da Internet. Lei 12.965/2014.** Coordenadores: Fabiano Dolenc Del Masso; Juliana Abrusio, Marco Aurélio Florêncio Filho. São Paulo: Editora Revista dos Tribunais, 2014. p.14.

HAJE, Lara**. Projeto do Senado de combate a notícias falsas chega à Câmara. Câmara dos Deputados, julho de 2020.** Disponível em: https://www.camara.leg.br/noticias/673694-projeto-do-senado-de-combate-anoticias-falsas-chega-a-camara. Acesso em: 22 de out. 2023.

HARARI, Yuval Noah**. 21 lições para o século 21.** São Paulo: Companhia das Letras, 2018.

HIRATA, A. (2017). **Direito à privacidade. Enciclopédia Jurídica da PUC-SP, edição 1.** Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 30 set. 2023.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016. 208 p.

KARRAS, T.; LAINE, S.; ALLA., T**. A Style-Based Generator Architecture for Generative Adversarial Networks.** 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach.

KOOPMAN, M., RODRIGUEZ, A. M.; GERADTS, Z. (2018). **Detection of Deepfake Video Manipulation.In: Conference: IMVIP, At Belfast. August 2018.** Recuperado de https://www.researchgate.net/publication/329814168_Detection_of_Deepfake_Video_Manipulation. Acesso 03 mar. 2023.

KORSHUNOV, P.; MARCEL, S. (2018**). Deepfakes: A new threat to face recognition? assessment and detection.** arXiv:1812.08685v1 [cs.CV] 20 Dec 2018. Recuperado de http://publications.idiap.ch/downloads/reports/2018/Korshunov_Idiap-RR-18-2018.pdf. Acesso 03 mar. 2023.

KOWALSKI, M. FaceSwap. **GitHub, 201**8. Disponível em: https://github.com/MarekKowalski/FaceSwap. Acesso em: 20 set. 2023.

LEITE, G. S.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas S.A. 2014.

LEMOS, André. **Plataformização, dataficação e performatividade algorítmica (PDPA): desafios atuais da cibercultura.** In: PRATA, N.; PESSOA, S. C. (org.). Fluxos comunicacionais e crise da democracia. São Paulo: Intercom, 2020.

LIMBERGER, Têmis. **Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático.** Revista de Direito Administrativo, v. 244, p. 248-263, 2007.

LONGO, Waldimir Pirró. **Tecnologia e soberania nacional São Paulo : Ed. Nobel**, 1984.

LOUBAK, A. L. **Aplicativo Zao usa deepfake para criar vídeos e viraliza na China.** TechTudo, 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/09/aplicativo-zao-usa-deepfake-para-criar-videos-e-viraliza-na-china.ghtml. Acesso em: 20 set. 2023.

MACGUILL, D. Libya Slavery. 2017. Disponível em: https://www.snopes.com/fact-check/libya-slavery. Acesso em: 28 ago. 2023.

MANNARA, B. (2022, 23 de maio). **Deepfake: golpistas usam vídeos com Elon Musk para negociar criptomoedas. Tilt***. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/05/23/deepfake-golpistas-usam-videos-com-elon-musk-para-negociar-criptomoedas.htm. Acesso em: 02 de out. de 2023.

MARINONI, Bruno; GALASSI, Vanessa. **Aspectos da desinformação, capitalismo e crises. In: MARTINS, Helena (org.). Desinformação: crise política e saídas democráticas para as *fake news*.** 1. ed. São Paulo: Editora Veneta, 2020.

MARTINS, A**. Na web, 12 milhões difundem *fake news* políticas.** 2017. Estadão. Disponível em: https://politica.estadao.com.br/noticias/geral,na-web-12-milhoes-difundem-fake-newspoliticas,70002004235. Acesso em: 20 de ago. de 2023.

MASSON, Cleber. Direito Penal: parte geral. 13. ed. Rio de Janeiro: Forense, 2019.

UTIDA, Mauro . Mídia NINJA. (2022, 19 de setembro). **Deepfake viraliza com pesquisa falsa na voz de Renata Vasconcellos no JN. Mídia NINJA**. Disponível em: https://midianinja.org/news/deepfake-viraliza-com-pesquisa-falsa-na-voz-de-renata-vasconcellos-no-jn. Acesso em: 03 e out. 2023.

MIRANDA, Rosângelo Rodrigues de. **A proteção constitucional da vida privada**. Imprenta: São Paulo, Led, 1996. p. 145/146.

MONTESQUIEU. **Do espírito das leis. Tradução de Jean Melville**. São Paulo: Martin Claret, 2003. Pág. 164.

MOROZOV, E. **Big Tech: a ascensão dos dados e a morte da política.** São Paulo: Ubu Editora, 2018.

NUCCI, Guilherme de Souza. **Manual de Direito Penal: 17 ed**. São Paulo: janeiro: Forense, 2021. 51 p.

O SENSACIONALISTA. 2023. Disponível em: https://oglobo.globo.com/blogs/humor/sensacionalista. Acesso em: 28 ago. 2023.

PACIEVITCH, Thais. **Tecnologia da informação e comunicação. 2014. Disponível em:**

PADILHA, Rodrigo. Direito constitucional: revista, atualizada e ampliada. 4. ed. São Paulo: Método, 2014. 660 p. 61.

PAESANI, Lilliana Minardi. **Direito e internet. Liberdade de informação, privacidade e responsabilidade civil. 6a edição**. Editora Atlas, São Paulo, 2013.

SANTAELLA, Lucia; SALGADO, Marcelo de Mattos. **Deepfake e as consequências**

sociais da mecanização da desconfiança. TECCOGS – Revista Digital de Tecnologias Cognitivas, n. 23, jan./jun. 2021. Disponível em: https://doi.org/10.23925/1984-3585.2021i23p90-103. Acesso em: 31 mai. 2023.

PARKER, G. G.; VAN ALSTYNE, M. W.; CHOUDARY, S. P. **Platform Revolution: How Networked Markets Are Transforming the Economy-and How to Make Them Work for You.** W. W. Norton & Company. 2016. Disponível em: http://103.44.149.34/elib/assets/buku/Platfrom_revolution.pdf. Acesso em: 03 ago. 2023.

PEREIRA, Danielly Ingrid Silva Almeida. (2020). **"Crimes contra a honra: calúnia, difamação e injúria!"** Recuperado de https://www.jusbrasil.com.br/artigos/crimes-contra-a-honra-calunia-difamacao-e-injuria/1116901225. Acesso em: 02 nov. 2023.

PINHEIRO, Patrícia Peck. Direito Digital. 5 ed. São Paulo: Saraiva, 2013.

PINTO, Kleber Couto. **A problemática das *fake news*. 2019.** 229 p. Disponível em: https://portal.estacio.br/media/4684338/kleber-couto-pinto.pdf. Acesso em: 22 out. 2023.

GROHMANN, Rafael. **Plataformização: fronteiras-estudos midiáticos. Fronteiras: Estudos Midiáticos, São Leopoldo, v. 22, n. 1, p. 1-10, 2020.** Disponível em: http://revistas.unisinos.br/index.php/fronteiras/article/view/fem.2020.221.01/60747734. Acesso em: 20 set. 2023.

POSTMAN, Neil, **Technopoly: the surrender of culture to technology. Vintage Books ed. New York, NY: Vintage Books,** 1993.

PRADO, Luiz Regis**. Curso de Direito Penal Brasileiro: Parte Geral e Parte Especial.** 18. ed. Rio de Janeiro: Forense, 2020.

PRATA, A. P**. O MARCO CIVIL DA INTERNET: PROTEÇÃO À PRIVACIDADE E INTIMIDADE DOS USUÁRIOS.** Universidade Federal de Uberlândia Faculdade de Direito Professor Jacy de Assis – FADIR. UBERLÂNDIA, p. 24 e 25. 2017. (78).

RAUPP, Eric. **Com potencial de destruir reputações, "deepfakes" se tornam acessíveis. Correio do Povo, 04 out. 2019.** Disponível em: https://www.correiodopovo.com.br/jornalcomtecnologia/com-potencial-de-destruirreputa%C3%A7%C3%B5es-*deepfakes*-se-tornam-acess%C3%ADveis-1.370284. Acesso em: 25 out. 2023.

MENESES, João Paulo. 2018. **Sobre a necessidade de conceptualizar o fenômeno das fake news**. Disponível em: https://doi.org/10.15847/obsOBS12520181376. Acesso em: 11 ago. 2023.

REINA, Eduardo**. Revista Consultor Jurídico, 8 de abril de 2023, 8h23.** Disponível em: https://www.conjur.com.br/2023-abr-08/china-cria-lei-informacoes-falsas-meio-*deepfakes*. Acesso em: 26 out. 2023.

RIGUES, Rafael**. Mulher é presa após criar deepfakes para prejudicar rivais da filha.** Revista Pesquisa FAPESP, 15 mar. 2021. Disponível em:https://olhardigital.com.br/2021/03/15/seguranca/mulher-e-presa-apos-criar-*deepfakes*-para-prejudicar-rivais-da-filha. Acesso em: 02 de out. de 2023.

RODRIGUES, Ricardo B. et al. **A cloud-based recommendation model. In: EURO AMERICAN CONFERENCE ON TELEMATICS AND INFORMATION SYSTEMS, 2014**.

SANTOS, Maria Celeste Cordeiro Leite dos. ARAÚJO, Marilene. **O tempo e o espaço. Fragmentos do marco civil da internet: paradigmas de proteção da dignidade humana.** Revista Bras. Políticas Públicas, Brasília. Vol. 7, nº 3. 2017.

SCHINK, Nina. **Deepfakes: The rise of digital propaganda. Oxford University Press.** 2019.

SCHMIDT, S. (2022, novembro). **Deepfakes: O Novo Estágio Tecnológico das Notícias Falsas (Edição 321).** Revista Pesquisa Fapesp. Disponível em: https://revistapesquisa.fapesp.br/deepfakes-o-novo-estagio-tecnologico-das-noticias-falsas. Acesso em: 02 de out. de 2023.

SENRA, Ricardo. **Na semana do impeachment, 3 das 5 notícias mais compartilhadas no Facebook são falsas.** 2016. BBC Brasil. Disponível em: https://www.bbc.com/portuguese/noticias/2016/04/160417_noticias_falsas_redes_brasil_fd. Acesso em: 10 out. 2023.

SÉRVIO, Gabriel. **“Quais são os sinais de um perfil falso nas redes sociais?”.** 2022. Disponível em: https://olhardigital.com.br/2022/04/29/tira-duvidas/sinais-perfil-falso-redes-sociais. Acesso em: 10 out. 2023.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** Ed., rev. E atual. São Paulo: Malheiros, 2005, p. 245-246.

SIQUEIRA, Dirceu P.; FERRARI, Caroline C. **O direito à informação como direito fundamental ao estado democrático. Revista Direitos Sociais e Políticas Públicas, v. 4, n. 2, p. 124-153, 2016**. Disponível em: http://www.unifafibe.com.br/revista/index.php/direitos-sociais-politicaspub/article/view/174. Acesso em: 01 abr. 2023.

SOLON, O. The **future of *fake news* : don’t believe everything you read, see or hear.** 2017. The Guardian. Disponível em: https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content. Acesso em: 30 ago. 2023.

SOUZA, Carlos Affonso. LEMOS, Ronaldo**. Marco Civil da Internet: Construção e Aplicação.** Juiz de Fora, MG: Editar Editora Associada Ltda, 2016; p.16.

SPADONI, Pedro. 2023. **Golpe com deepfake na China dispara alerta contra IA. Olhar Digital.** Disponível em: https://olhardigital.com.br/2023/05/22/seguranca/golpe-com-deepfake-na-china-dispara-alerta-contra-ia. Acesso em: 02 out. 2023.

STEENSMA, H. Kevin. **Acquiring technological competencies through inter-organizational collaboration: an organizational learning perspective. Journal of Engineering and Technology Management,** v. 12, 1996. Disponível em: https://doi.org/10.1016/0923-4748(95)00013-5. Acesso em: 04 out. 2023.

SUNDFELD, Carlos Ari**. Princípio da publicidade administrativa (Direito de certidão, vista e intimação).** Revista de Direito Administrativo, v. 199, p. 97-110, 1995.

SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. Imprenta: São Paulo, Revista dos Tribunais, 2005. p. 153.

TANDOC JR., E.; LIM, Z.W., LING, R. 2017. **Defining "*Fake news* ": A Typology of Scholarly Definitions.** Digital Journalism, London.

THIES, J. et al. **Face2Face: Real-Time Face Capture and Reenactment of RGB Videos**. 2016. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas.

TOLOSANA, R. et al. Deepfakes and Beyond: **A Survey of Face Manipulation and Fake Detection**. Journal of Latex Class Files, Madri, v. XIII, n. 9, 1 Março 2016.

RAPHAEL, Pablo. UOL. 2018. **A Disney pode recriar Carrie Fisher no próximo Star Wars, mas não vai**. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/01/04/a-disney-pode-recriar-carrie-fisher-no-proximo-star-wars---mas-nao-vai.htm. Acesso em: 10 de ago. 2023.

VACCARI, Cristian. **Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News**. 2020. Disponível em: https://doi.org/10.1177/2056305120903408. Acesso em: 01 nov. 2023.

VENOSA, Sílvio de Salvo. **Direito civil: obrigações e responsabilidade civil**. 17. ed. São Paulo: Atlas, 2017.

VILHA, Anapatrícia Morales; Di Agustini, Carlos Alberto**. E-marketing para bens de consumo duráveis**. Rio de Janeiro. Editora FGV. 2002.

VIZOSO, Ángel, VAZ-ÁLVAREZ, Martín e LÓPEZ-GARCÍA, Xosé. Fighting Deepfakes: **Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. Media and Communication;** vol. 9, n. 1, p. 291-300, 03 mar. 2021.

Disponível em: http://dx.doi.org/10.17645/mac.v9i1.3494. Acesso em: 01 nov. 2023.

WANG, P. **This Person does not Exist. This Person does not Exist,** 2019. Disponível em: https://thispersondoesnotexist.com. Acesso em: 20 set. 2023.

WARDLE, C. *Fake news*. **It's complicated.** 2017. On-line. Disponível em: https://firstdraftnews.org/articles/fake-news-complicated. Acesso em: 20 de ago. de 2023.

WEST, J.; BERGSTROM, C. Home. **Which Face is Real?,** 2019. Disponível em: https://www.whichfaceisreal.com/index.php. Acesso em: 20 set. 2023.

ZATTI, D. **Polícia Federal quer saber os motivos para Dilma doar R$30 Bilhões a Friboi. 2016.** On-line. Disponível em: https://pensabrasil.com/policia-federal-quer-saber-os-motivos-para-dilmadoar-r-30-bilhoes-a-friboi. Acesso em: 19 ago. 2023.