FACULDADE EVANGÉLICA DE GOIANÉSIA

CURSO DE DIREITO

GABRIEL ADORNO MOTA

JOÃO PAULO DA CUNHA

DEEPFAKE E O PROCESSO ELEITORAL: O PODER DE MANIPULAÇÃO DA INTELIGÊNCIA ARTIFICIAL FRENTE A LEGISLAÇÃO BRASILEIRA

GOIANÉSIA/GO

2023

GABRIEL ADORNO MOTA

JOÃO PAULO DA CUNHA

DEEPFAKE E O PROCESSO ELEITORAL: O PODER DE MANIPULAÇÃO DA INTELIGÊNCIA ARTIFICIAL FRENTE A LEGISLAÇÃO BRASILEIRA

Artigo Científico apresentado como Trabalho de Conclusão de Curso, apresentado à Faculdade Evangélica de Goianésia (FACEG), em nível bacharel, como requisito parcial para a obtenção do grau de Bacharel em Direito.
Orientador: Prof. Me. Carlos Alberto da Costa

GOIANÉSIA/GO

2023

FOLHA DE APROVAÇÃO

Este artigo foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO – FACEG.

Aprovado em, 04 de julho de 2023.

Nota Final 65.

Banca examinadora:

Prof. Me. Carlos Alberto da Costa

Orientador

Prof.ª Me. Cristiane Ingrid de Souza Bonfim

Professora convidada

Prof.ª Esp. Luana de Miranda Santos

Professora convidada

DEEPFAKE E O PROCESSO ELEITORAL: O PODER DE MANIPULAÇÃO DA INTELIGÊNCIA ARTIFICIAL FRENTE A LEGISLAÇÃO BRASILEIRA

DEEPFAKE AND THE ELECTORAL PROCESS: THE MANIPULATION POWER OF ARTIFICIAL INTELLIGENCE IN BRAZILIAN LEGISLATION

GABRIEL ADORNO MOTA

JOÃO PAULO DA CUNHA

Resumo: O presente trabalho tem como tema "*Deepfake* e o Processo Eleitoral: O poder de manipulação da inteligência artificial frente a legislação brasileira". Quanto ao objetivo geral, pretende-se demonstrar a ameaça dos *deepfakes* ao sistema democrático brasileiro. Referente aos objetivos específicos, pretende-se analisar os aspectos históricos e conceituais de deepfakes sob a ótica das legislações brasileiras; e interpretar o dever preventivo do Estado com a adoção da Convenção de Budapeste no combate aos *deepefakes.* A metodologia adotada na investigação torna possível classificar a presente pesquisa, quanto aos meios, como sendo bibliográfica e quanto aos seus fins, trata-se de uma pesquisa exploratória. No tocante a problemática está se origina da seguinte pergunta: Os Deepfakes como recente inovação tecnológica no sistema eleitoral brasileiro pode ser combatida com as legislações em vigor no território nacional? Os principais autores utilizados para responder à pergunta acima elucidada foram CITRON (2019), CASTELLS (2013), MOURA (2019) e CASTRO (2003). Depreende-se, portanto, que o combate ao '*DeepFake'* ganhou reforço e se concretizou em território nacional, após a adesão do Brasil como signatário da convenção do 'Cibercrime', popularmente conhecida como Convenção de Budapeste. Pois a partir da pactuação ao Decreto-lei 11.491 de 12 de abril de 2023, é possível uma política criminal comum entre os signatários, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional.

Palavras-chave: *DeepFake*. Democracia. Direito Eleitoral. Legislação Brasileira

Abstract: The present work has as its theme "Deepfake and the Electoral Process: the power of manipulation of artificial intelligence in the face of Brazilian legislation". As for the general objective, it is intended to demonstrate the threat of deepfakes to the Brazilian democratic system. Regarding the specific objectives, it is intended to analyze the historical and conceptual aspects of deepfakes from the perspective of Brazilian legislation; and interpret the preventive duty of the State with the adoption of the Budapest Convention in combating deepfakes. The methodology adopted in the investigation makes it possible to classify the present research, in terms of means, as being bibliographical and in terms of its purposes, it is an exploratory research. Regarding the problem, it originates from the following question: Can Deepfakes as a recent technological innovation in the Brazilian electoral system be combated with the legislation in force in the national territory? The main authors used to answer the question elucidated above were CITRON (2019), CASTELLS (2013), MOURA (2019) and CASTRO (2003). It appears, therefore, that the fight against 'Deep Fake' gained strength and took place in the national territory, after Brazil joined as a signatory to the 'Cybercrime' convention, popularly known as the Budapest Convention. Since the agreement to Decree-Law 11,491 of April 12, 2023, a common criminal policy between the signatories is possible, with the objective of protecting society against crime in cyberspace, namely, through the adoption of adequate legislation and the improving international cooperation.

Keywords: DeepFake. Democracy. Electoral Law.Brazilian legislation.

INTRODUÇÃO

O presente trabalho tem como tema "*Deepfake* e o Processo Eleitoral: o poder de manipulação da inteligência artificial frente a legislação brasileira. Neste prisma, os avanços da inteligência artificial e o surgimento de novas técnicas como *deepfake* possibilitam a manipulação e criação de novos conteúdos falsos de vídeos, áudios e imagens muito semelhantes ao conteúdo original, apesar de trazer diversos benefícios, seu uso indevido é preocupante, os deepfake se tornaram uma ferramenta poderosa para influenciar ou distorcer a verdade, seja no âmbito político ou social, usada dessa forma a tecnologia passa a ser uma extensão das fake News.

Justifica-se a escolha da temática devido a sua relevância jurídica e social. Quanto a importância jurídica do tema, é imprescindível o debate devido a ofensa ao direito à imagem, à veiculação e divulgação de notícias falsas, e a mais nova atualização legislativa com o Decreto-lei 11.491 de 12 de abril de 2023, que incorpora a Convenção de Budapeste no ordenamento jurídico brasileiro; isso porque a partir do momento em que se há a discussões de parâmetros na legislação o debate no âmbito jurídico se torna elementar para apontamentos críticos e atualização acerca do conteúdo. Referente a relevância social, no entanto, vê-se que no contexto dos processos eleitorais, os deepfakes podem ser utilizados como ferramentas de desinformação e manipulação da opinião pública.

Ademais, deve-se considerar que o objetivo geral da pesquisa pretende suscitar a ameaça das deepfakes ao sistema democrático brasileiro. No que tange os objetivos específicos, no entanto, pretende-se analisar os aspectos históricos e conceituais de deepfake sob a ótica das legislações brasileiras; e interpretar o dever preventivo do Estado com a adoção da Convenção de Budapeste no combate aos deepefakes.

Para isso, a metodologia adotada na investigação torna possível classificar a presente pesquisa, quanto aos meios, como sendo bibliográfica e quanto aos seus fins, trata-se de uma pesquisa exploratória, por meio de indicações extraídas da legislação, das jurisprudências, de doutrinas jurídicas e artigos científicos que versam sobre o conteúdo em análise. Não obstante, a problemática da presente pesquisa gira em torno da seguinte indagação: As

Deepfakes como recente inovação tecnológica no sistema eleitoral brasileiro pode ser combatida com as legislações em vigor no território nacional?

Os principais autores no percurso teórico são: Citron (2019), Castells (2013), Moura (2019) e Castro (2003). Outrossim, a estruturação do artigo segue a ordem dos objetivos acima indicados, ou seja, inicialmente, no primeiro tópico será abordado questões voltadas ao *Depeefake,* quanto a sua origem e natureza jurídica, paralelamente, far-se-á análises aos aspectos históricos e evolutivos à luz das legislações brasileiras.

Em seguida, no segundo tópico, suscitará vieses referentes aos deepfakes no sistema eleitoral democrático de modo a compreender os impactos causados a democracia com o uso da inteligência artificial e, por fim, no terceiro tópico se discutirá sobre dever preventivo do Estado com adesão do brasil à convenção de Budapeste (Decreto 11.491 de 12 de abril de 2023), em relação a (in)aplicabilidade do direito internacional nos ciberespaços. Logo, pretende-se uma compreensão clara e coesa acerca do tema, não só para o âmbito acadêmico, mas também para todos os eventuais leitores.

1 DEEPFAKES: ASPECTOS HISTÓRICOS E EVOLUTIVOS À LUZ DAS LEGISLAÇÕES BRASILEIRAS

Inicialmente, é elementar destacar que, em 2017 a rede social virtual Reddit, teve o primeiro caso de *deepfake* quando um usuário divulgou vídeos falsos nos quais atrizes de Hollywood tiveram seus rostos inseridos em vídeos de conteúdo adulto, impróprio aos menores, como por exemplo, material pornográfico (MOURA,2019). Neste caso, a inteligência artificial foi utilizada para produzir e editar um conteúdo falso, algo que até então, não havia acontecido.

Não obstante, a partir dessa perspectiva que alicerça a expressão *deepfake,* se tratando de uma mescla dos termos de língua inglesa *deeplearning* (aprendizagem profunda) e fakes (falso), entrou há alguns anos no repertório da web e na cultura popular, suscitando preocupação e provocando as empresas digitais a se prepararem para um futuro com áudios e vídeos forjados ao sabor da criatividade humana e da capacidade do aprendizado de máquina.

Sendo assim, a tecnologia do *deepfake* usa o algoritmo Deep Learning na elaboração de conteúdos falsos, criando situações embaraçosas e

disseminando conteúdo e informações falsas. Isso porque, os deepfakes não atuam somente em sites de conteúdo adulto, as implicações do uso desta tecnologia conforme esclarecem Young (2019) “podem causar situações muito piores quando associadas à política, à veiculação de notícias falsas”, causando na população mundial um sentimento de instabilidade e ceticismo ao ver ou ouvir essas notícias em seu cotidiano”.

Salienta-se, contudo, que em 2018, a expressão *deepfake* obteve outras técnicas associadas ao seu nome, como por exemplo: reconstituição da expressão facial, manipulação de corpo inteiro e plano de fundo e síntese de áudio, nesse sentido leciona Spencer (2019, p. 57)

> Nesse novo mundo, a IA é capaz de mimetizar conteúdo humano, e tem o potencial de ser usada por maus atores, e campanhas financiadas por Estados, para influenciar os sentimentos da população de várias formas. Estamos testemunhando uma explosão de fraude online. [...] Personagens e textos fakes são os próximos fronts do debate em torno do deepfake, que está só começando e é ainda outra maneira com a qual a inteligência artificial pode ser aproveitada como máscara e alterar o sentimento coletivo através de truques digitais [...]. Humanos digitais, âncoras de jornais de inteligência artificial, personas virtuais tudo é possível na nova internet. O mercado de farsa online já está maduro.

Nessa perspectiva, realça-se ainda que em 2019, a ONG francesa *Solidarité* SIDA (AIDS *Solidarity*) publicou um *deepfake* em que o presidente dos Estados Unidos, Donald Trump, afirmava que a AIDS havia sido erradicada. Nesse sentido o intuito da campanha, intitulada *“The DeepFake News Campaign*”, era chamar atenção para o combate à doença através da grande quantidade de compartilhamentos que a postagem alcançaria nas redes sociais. Além de atingir a reputação e a trajetória dos indivíduos diretamente envolvidos, tais materiais ajudam a propagar mentiras e a gerar “graves consequências governamentais e diplomáticas”. (LEAL,2020)

Percebe-se, contudo, que apesar de soarem como reais, deepfakes são criadas a partir de tecnologias de *deeplearning*, que realizam a edição de pixels ou sons e, então, forjam até mesmo a criação de rostos em filmes e de vozes em gravações preexistentes. Não obstante, a alteração realística e em tempo real pode criar vídeos fantásticos a um baixo custo, mas também provocar danos incríveis. Trata-se de uma expressão majoritariamente usada para descrever

qualquer conteúdo de vídeo que aparenta ser realista, e, na verdade, é falsificado.

Conforme elucida, Teixeira (2016), não tardou, portanto, que a tecnologia fosse descrita por uma infinidade de notícias que apontam suas implicações mais nefastas, como o potencial de uso na produção de propaganda falsa, “tanto para a criação de perfis falsos em redes sociais e até em campanhas de difamação”.

Congruente ao indicado, a inteligência artificial possui duas categorias de algoritmos denominadas Machine Learning (ML) e Deep Learning (DL ou Rede Neural Profunda) (GUILLOU, 2018). Desta maneira, o Deep Learning é um algoritmo que aprende com seus erros. E esta explicação relaciona-se aos deepfakes, conforme elucidação de Spencer (2019, p.59), em seu artigo intitulado “*DeepFake*, a mais recente ameaça distópica”, descreve:

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

Em um panorama brasileiro, importa-se enfatizar, que até o ano de 2012, não havia legislação específica para punir os crimes cibernéticos próprios. Apesar disso, a primeira proposta de regulação aprovada na Câmara foi o PL 84/99, também conhecido como PL dos Crimes Digitais, de autoria do deputado Luiz Piauhylino. “O projeto considerava crimes a invasão e alteração de conteúdos de sítios, o roubo de senhas e a criação e disseminação de vírus”. (BRASIL, 2015, p.7).

Cumpra-se mencionar que, tencionando coibir a prática dos crimes informáticos, foi sancionada, no ano de 2012, a lei 12.735, popularmente conhecida como Lei Azeredo. Oriunda do projeto de lei da Câmara dos Deputados de nº 84 de 1999, a proposição visava à inclusão de diversas tipificações no Código Penal (1941), que não foram aprovadas; entretanto, a expertise da polícia judiciária foi incluída após substitutivo oriundo do Senado

Federal. Tramitando por longos treze anos e após diversas modificações, submeteu-se o aludido projeto de lei à sanção presidencial.

À luz de Dias (2021), a lei trouxe como inovação prática no que concerne ao preparo das Polícias Judiciárias para o combate dos crimes digitais (estímulo da criação de delegacias de crimes digitais). Esta lei por vezes, é rediscutida no Congresso Nacional, pois em sua propositura inicial previa várias condutas incriminadoras a fim de tipificar crimes digitais, que foram decotadas do texto e hoje carecem de regulamentação legal. Destarte, outra inovação legislativa se deu no ano de 2012 com o advento da Lei federal n.º 12.737/2012 – lei Carolina Dieckmann. Importante destacar que, a nova lei ganhou notoriedade porque, antes mesmo de publicada e sancionada, já havia recebido o nome de "Lei Carolina Dieckmann[1]".

> esta lei, recebeu referida denominação em decorrência de que durante a sua tramitação no Congresso Nacional, a atriz Carolina Dieckmann teve sua vida íntima publicada e divulgada sem seu consentimento e autorização nas redes sociais, violando totalmente o direito a intimidade. Direito este, constituído legalmente a todo o ser humano na Constituição Federal, a qual repousa no artigo 5º, inciso X, nos seguintes termos: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]". (BRASIL, 1988, p. 3).

Deve-se explanar que, a referida lei, pela primeira vez no direito brasileiro, dispõe sobre a tipificação criminal de delitos informáticos, que estabelece princípios, garantia, direito e deveres quanto ao uso da internet, permitindo a responsabilização penal dos infratores, vez que até então o Código Penal não possuía artigos que tratassem especificamente de crimes eletrônicos. A principal inovação é que foram acrescentados ao Código Penal, por meio da lei em questão, os artigos 154-A e 154-B, e foram alterados os artigos 266 e 298. (BRASIL, 1941).

Neste viés, aufere-se que o artigo 154-A tipifica o crime de invasão de dispositivo informático, seja este conectado ou não à rede de computadores, através de violação de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo. Nestes termos,

[1] Carolina Dieckmann Worcman é uma atriz brasileira. A Lei Carolina Dieckmann é como ficou conhecida a Lei Brasileira 12.737/2012, sancionada em 30 de novembro de 2012 pela então presidente Dilma Rousseff, que promoveu alterações no Código Penal Brasileiro, tipificando os chamados delitos ou crimes informáticos.

segundo Ferreira (2015) no caso de invasão para obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais ou informações sigilosas a pena é mais grave: “de seis meses a dois anos de reclusão, além de multa, isso caso a conduta não constitua crime mais grave”.

Outrossim, a lei prevê também outras causas específicas de aumento de pena, como, por exemplo, se o crime for praticado com presidente da República, governadores, prefeitos, entre outros previstos no rol taxativo do parágrafo 5º. Nas palavras de Capez (2013), artigo 154-B estabelece que a Ação Penal para as condutas trazidas pelo artigo anterior somente se procede mediante representação do ofendido, qual seja, daquele que teve seu dispositivo violado, salvo se o crime for cometido contra a administração direta ou indireta de qualquer dos poderes da União, estados, Distrito Federal ou municípios ou ainda contra empresas concessionárias de serviços públicos. Nesses casos específicos a Ação Penal será pública incondicionada. (BRASIL,1941).

Noutro giro, a lei do Marco Civil da Internet (Lei n° 12965, de 23 de abril 2014), trata-se de uma lei ordinária federal que foi sancionada em 2014, pela então presidente Dilma Rousseff, visa a constituição da internet, isso se deve ao fato de que se trata de uma lei de cunho principiológico, onde sua principal funcionalidade é estabelecer princípios, deveres, valores, direitos e garantias referente ao uso da internet no Brasil. Outrossim, é oportuno considerar que o Marco Civil da Internet foi votado com o objetivo de pautar as ações realizada na Internet no mundo jurídico:

> Definida como “Constituição” da Internet, referido texto normativo veio a aprimorar e delimitar o uso da Internet no Brasil, de modo a conferir maior garantia dos direitos advindos da rede, bem assim, mais direitos e deveres aos usuários, como *“novatio legis’* especial de regulamentação detalhada e precisa dos direitos da Internet. (NEVES; VANCIM, 2015)

Destarte, Recuero (2009, p. 24) destaca que o Marco Civil, empenhou-se em assegurar mecanismos que possibilitem uma conexão mais segura,” com especial atenção a proteção ao direito à privacidade, intimidade e liberdade de expressão, deixando claro, que o espaço virtual não é espaço de impunidade”. Contudo, anteriormente ao projeto de lei em questão, tramitava o projeto de Lei Azevedo que previa criminalizar condutas tidas como corriqueiras por muitas

pessoas, no entendimento de Habermas (HERMANN, 2014, p. 92), “dessa forma apresentava muitas falhas, tornando o texto de lei demasiadamente amplo e por fim engessaria todo o seu funcionamento”.

Deflagra-se, que para não provocar o mesmo equívoco, percebeu-se que antes de tratar da regulamentação criminalmente da internet, o projeto do Marco Civil preocupou em definir os direitos civis tendo como base os princípios fundamentais elencados na Constituição Federal 1988. Com isso, a redação sistematizou seus pilares na Neutralidade da Rede, na Liberdade de Expressão e na Privacidade. (BRASIL,2014)

Dentro do contexto eleitoral, além do Marco Civil, a regulação das redes sociais também está sujeita ao Código Civil Eleitoral e as Resoluções publicadas pelo Tribunal Superior Eleitoral (TSE). Especificamente sobre o último pleito, as Leis nº 13.487 e 13.488, editadas em 2017 (BRASIL, 2017a, 2017b), produziram o que se costuma denominar de minirreforma eleitoral, provocando alterações importantes nas Leis nº 9.504/97 (Lei das Eleições), nº 9.096/95 (Lei dos Partidos Políticos) e no Código Eleitoral (Lei nº 4.737/65). No que tange a comunicação política e a liberdade de expressão, a Lei 13.487/2017 passa a permitir o impulsionamento de conteúdo nas redes sociais como parte da propaganda eleitoral do candidato, antes vedada. (BRASIL, 2014)

Neste aspecto, importa indicar o Decreto nº 11.491 de 12 de abril de 2023, o decreto presidencial pelo qual fica formalmente aprovada a adesão do Brasil à Convenção de Budapeste, um tratado internacional sobre crimes cibernéticos. Essa referida convenção consiste em um ordenamento desenvolvido pelo Conselho da Europa em 2002, em que seu objetivo girava em torno da proteção da sociedade contra a criminalidade no ciberespaço.

Não obstante, é elementar assinalar que a Convenção de Budapeste promovia a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, mas atualmente encontra-se aberta à assinatura por todos os países que a desejarem, tendo em vista que os crimes cibernéticos atingem todos os territórios do mundo. (FERNANDES, 2013)

No Direito Internacional, existe o Direito Internacional Uniforme, utiliza por quase todos os países do mundo, que ocorre quando coincidem os direitos primários entre ordenamentos, seja porque têm a mesma origem, ou por sofrerem influências idênticas, ou, ainda, quando países adotam sistemas

jurídicos clássicos total ou parcialmente, de outros Estados (FERNANDES, 2013). Ademais, segundo indica Furquim (2023), a integral implementação da Convenção de Budapeste no Brasil trará resultados positivos ao país, uma vez que ensejará a modernização de normativos e políticas adotadas na temática de enfrentamento aos crimes cibernéticos, assim como na coleta e preservação das provas digitais.

Observa-se, que além do aperfeiçoamento da cooperação internacional na instrução e elucidação dos delitos praticados no ambiente virtual, a Convenção também impulsiona o Brasil a dar continuidade ao desenvolvimento de seu ordenamento jurídico e de sua política diante do avanço da criminalidade no ambiente cibernético, assim o fazendo com o devido equilíbrio entre a intensificação da persecução penal e a proteção de dados pessoais. Desta forma, deve-se, a posteriori, realizar análises quanto as deepfakes no sistema eleitoral democrático, de modo a compreender os impactos causados a democracia com o uso da inteligência artificial.

2 DEEPFAKES NO SISTEMA ELEITORAL DEMOCRÁTICO: QUANDO OS OLHOS DEIXAM DE SER TESTEMUNHAS CONFIÁVEIS

Inicialmente, é elementar indicar que apoiados em técnicas de inteligência artificial e aprendizado de máquina, capazes de manipular conteúdo de áudio e vídeo de maneira convincente, os deepfakes conseguem criar experiências que podem facilmente se passar como verdade. De acordo com Citron (2019), definir o que é real e o que é falso está cada vez mais trabalhoso no ambiente digital.

Nestes moldes, o hiper-realismo e a qualidade visual dos deepfakes, aliados a olhos pouco treinados ou que desconhecem a tecnologia, tornam quase impossível, em alguns casos, distinguir um *deepfake* de um material autêntico. De acordo com pesquisa recente da empresa de segurança digital Kaspersky (CNN,2019), 66% dos brasileiros não sabem o que é um *deepfake*, enquanto 7 em cada 10 não saberiam reconhecer um vídeo que tenha utilizado a técnica inovadora.

Conforme destaca Assolini (2019, p.265), o fato de a maioria das pessoas estar predisposta a acreditar em um vídeo ou áudio criado digitalmente, “por não saberem que é possível fazer tal coisa, facilita o êxito de campanhas de

desinformação ou golpes online que utilizem tais técnicas de deepfake". Neste sentido, é oportuno, constar que apesar de silenciosas, as *deepfakes* trazem inúmeros prejuízos à sociedade, principalmente à democracia.

Tão logo, com a facilidade na disseminação de notícias e na manipulação delas, os governos autoritários se utilizam desse artifício para obter aprovação popular, por meio de um discurso e aparência mentirosa de um governo democrático. Para Castells (2009), no contexto histórico que se vive, a política consiste majoritariamente na política midiática. Uma vez que os meios de comunicação constituem a nova ágora na qual relações de poder são disputadas e estabelecidas, basicamente todos os atores políticos e sociais precisam buscar seu espaço na mídia, a fim de se fazerem ouvir e alcançarem seus objetivos, pois:

> em virtude dos efeitos convergentes da crise dos sistemas políticos tradicionais e do grau de penetrabilidade bem maior dos novos meios de comunicação, a comunicação e as informações políticas são capturadas essencialmente no espaço da mídia. Tudo o que fica de fora do alcance da mídia assume a condição de marginalidade política. (Castells, 2018, p. 944)

Por outra perspectiva, de acordo com Leal (2020), mas um feito impactante das deepfakes é o efeito negativo na credibilidade e autenticidade em toda e qualquer mídia divulgada, pois gera descredito a massa populacional, em vista de que aquela informação pode não ser genuína e indistinguível do conteúdo original.

Neste interim, a questão que assume fulcral importância reside no fato empiricamente comprovado de que a criação e disseminação de deepfakes tem capacidade potencial de influenciar o resultado de um pleito eleitoral, atingindo o Estado Democrático de Direito em sua essência: a emanação do poder pelo povo, no exercício da escolha de seus representantes políticos, que consiste em Cláusula Constitucional Pétrea (parágrafo único do artigo 1º, da Constituição Federal). (BRASIL,1988, online)

Nesta perspectiva, é oportuno salientar que no que diz respeito a esse contexto eleitoral a situação se agrava, uma vez que há a polarização de ideologias políticas, não havendo, desse modo, a análise lógica das informações que recebemos, posto que somos facilmente convencidos de qualquer informação negativa sobre aquilo que é antagônico ao que defendemos é

verdadeiro. Conforme elucida Gomes (2018), se torna mais fácil manipular a opinião pública para determinado resultado pretendido.

Paralelamente, é indispensável mencionar que embora a disputa pelo poder seja uma característica intrínseca à própria política, sobretudo em se tratando de sistemas democráticos, e embora a comunicação seja um fenômeno tão antigo quanto a humanidade em si, há um fator relativamente novo que deve ser levado em consideração quando pensamos o debate político atualmente (MOURA,2019).

Noutro giro, trata-se do surgimento da autocomunicação em massa, um processo de transformação tecnológica e organizacional da comunicação, “baseada em redes horizontais de comunicação multidirecional, interativa, na Internet; e, mais ainda, nas redes de comunicação sem fio, atualmente a principal plataforma de comunicação em toda parte”. (Castells, 2013, p. 128)

Tão logo, contribui Benkler (2006) ao indicar que, vivemos em uma esfera pública conectada, que permite que os “indivíduos, atuando sozinhos ou com outros, sejam participantes ativos da esfera pública, em vez de leitores, ouvintes ou espectadores passivos” (Benkler, 2006, p. 212). As pessoas tomam decisões, incluindo-se aquelas relacionadas à política, baseadas em informações, e sobretudo imagens, que são produzidas e divulgadas pela mídia tradicional e na Internet. (Castells, 2009)

Nestes termos, as imagens com as quais se tem contato geram um primeiro reflexo emocional, que é seguido de um processo cognitivo de elaboração e decisão; “a impressão do contato inicial se transforma em opinião, a qual, por sua vez, se confirma ou se desmente na elaboração do debate contínuo que acontece nas redes sociais em interação com a mídia” (Castells, 2018, p.253). Outra questão a ser considerada é que enquanto compartilhar uma informação é extremamente fácil, corrigir uma informação incorreta que foi compartilhada é muito mais difícil (WESTERLUND, 2020), lógica que se aplica às *deepfakes.*

Neste aspecto, salienta-se que na maioria das vezes, o alcance da informação verídica ou ajustada não é o mesmo que obteve o boato ou a desinformação; em muitas outras, a correção pode ser inapta para sanar o dano causado inicialmente. Basta imaginar a hipótese em que uma *deepfake* retratando determinado candidato seja divulgada às vésperas da eleição à qual

está concorrendo. (CITRON; CHESNEY, 2019). Em que pese a Lei Eleitoral não tratar diretamente sobre as notícias falsas, disciplina sobre a sanção aplicada aos grupos responsáveis por disseminar conteúdo que atinja a honra de candidato, partido ou coligação. A título de exemplo podemos citar:

> Art. 57-H. Sem prejuízo das demais sanções legais cabíveis, será punido, com multa de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais), quem realizar propaganda eleitoral na internet, atribuindo indevidamente sua autoria a terceiro, inclusive a candidato, partido ou coligação. (Incluído pela lei 12.034/09). § 1º Constitui crime a contratação direta ou indireta de grupo de pessoas com a finalidade específica de emitir mensagens ou comentários na internet para ofender a honra ou denegrir a imagem de candidato, partido ou coligação, punível com detenção de 2 (dois) a 4 (quatro) anos e multa de R$ 15.000,00 (quinze mil reais) a R$ 50.000,00 (cinquenta mil reais). (Incluído pela lei 12.891/13) § 2º Igualmente incorrem em crime, punível com detenção de 6 (seis) meses a 1 (um) ano, com alternativa de prestação de serviços à comunidade pelo mesmo período, e multa de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais), as pessoas contratadas na forma do § 1º. (BRASI, 1997)

Para Castells (2009), no contexto histórico em que vivemos, a política consiste majoritariamente na política midiática. Uma vez que os meios de comunicação constituem o nova agora na qual relações de poder são disputadas e estabelecidas, basicamente todos os atores políticos e sociais precisam buscar seu espaço na mídia, a fim de se fazerem ouvir e alcançarem seus objetivos. Outrossim, importante destacar a Resolução 23.551 5 do TSE que fala sobre as implicações jurídicas a respeito das propagandas eleitorais contendo inveracidades:

> Art. 22. É permitida a propaganda eleitoral na internet a partir do dia 16 de agosto do ano da eleição (lei 9.504/97, art. 57-A).
> § 1º A livre manifestação do pensamento do eleitor identificado ou identificável na internet somente é passível de limitação quando ocorrer ofensa à honra de terceiros ou divulgação de fatos sabidamente inverídicos.
> § 2º O disposto no § 1º se aplica, inclusive, às manifestações ocorridas antes da data prevista no caput, ainda que delas conste mensagem de apoio ou crítica a partido político ou a candidato, próprias do debate político e democrático. (BRASIL,1997)

Não obstante, a desinformação pode operar por meio de publicidade pública de certo regime política, ou por meio da publicidade privada, por meio de boatos, sondagens e estatísticas, filtragem de informações ou estudos supostamente científicos e imparciais. Desta maneira, complementa Moura (2019), que a desinformação é a utilização de técnicas de comunicação e

informação para induzir a erro ou dar uma falsa imagem da realidade mediante a supressão ou ocultação de informações, minimização de sua importância ou modificação do seu sentido.

Em 2018, com o objetivo de combater os efeitos da propagação da *depeefake* e *fake news* sobre as eleições, o Tribunal Superior Eleitoral (TSE) criou o Sistema de Alerta de Desinformação Contra as Eleições. Nesse sistema é possível comunicar à Justiça Eleitoral o recebimento de notícias falsas, descontextualizadas ou manipuladas sobre o processo eleitoral brasileiro. Deve-se dar ênfase a criação, em 24 de maio de 2019, pelo TSE, da Portaria 3826, na qual institui grupo de trabalho incumbido de elaborar propostas de novas linhas de ação do Tribunal Superior Eleitoral sobre desinformação e eleições. (BRASIL,2019, *online*).

Destarte, como uma tentativa de barrar a disseminação das deepefakes e Fake News e proporcionar uma campanha eleitoral ética e justa, foram desenvolvidos alguns sistemas de identificação de notícia falsa. Tão logo, observa-se que no site do Tribunal Eleitoral do Estado do Rio Grande do Sul (TRE-RS,2022), por exemplo, existe uma seção que trata sobre o enfrentamento à desinformação eleitoral, onde está disponível o número de WhatsApp, bem como e-mail, nos quais os eleitores podem enviar comunicados referente às eleições e, a partir disso, o Tribunal analisa a informação, para saber se é verdadeira ou mais um *deepefake* disseminada na internet.

Ademais, o site da Justiça Eleitoral possui diversos conteúdos informativos acerca do assunto, auxiliando a população a identificar uma notícia falsa. (JUSTIÇA ELEITORAL, 2022). Em consonância ao delineado, para que haja um processo eleitoral democrático, é imprescindível que a formação do convencimento do eleitor seja livre, isenta de quaisquer tipos de manipulações. E é por esse motivo, que a Justiça Eleitoral e o Poder Legislativo devem adotar medidas profiláticas no sentido de assegurar que as redes sociais serão utilizadas “como instrumento diálogo legítimo, de participação popular, liberto do impacto negativo da desinformação, tão recorrente com o advento das rápidas transformações tecnológicas”. (DIAS, 2018, p.37).

Destarte, deve-se, à frente, analisar a novação legislativa sob o Decreto Decreto-lei nº 11.491 de 12 de abril de 2023, que incorpora a Convenção de Budapeste no ordenamento jurídico brasileiro; bem como fazer apontamentos

que alicerçam a problemática do presente artigo, isto é, traçar constatações acerca da responsabilidade e combate das deepefakes frente ao arcabouço legislativo em vigência no país.

3 A (IN)APLICABILIDADE DO DIREITO INTERNACIONAL NOS CIBERESPAÇOS: UMA AVALIAÇÃO SOBRE O PROCESSO DE ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE (DECRETO 11.491 DE 12 DE ABRIL DE 2023)

Referente a problemática suscitada pela presente pesquisa, é crucial realizar apontamentos sobre a capacidade de combate as depeefakes com as legislações em vigor no território nacional. Nesta perspectiva, deve-se realçar, que para a doutrina em geral existe a classificação dos cibercrimes em duas grandes modalidades, os impróprios e os próprios. Os impróprios são os “tradicionais”, são os crimes comuns (à exemplo do furto, estelionato etc.) que utilizam a rede de computadores como meio para praticar outros crimes. Já os delitos próprios, são aqueles nos quais a informática não é simplesmente objeto do crime, são os delitos contra as próprias redes de computadores (VINÍCIUS, 2013, *online*).

Tão logo, deve-se realçar que os prejuízos com cibercrimes no Brasil já alcançam, no ano de 2016, US$10,3 bilhões segundo uma pesquisa anual intitulada Norton Cyber Security Insights Report (NORTON, 2016, online). Isso, portanto, deixa o Brasil como quinto país com maior número de vítimas dos crimes pela internet. De acordo com o relatório anual, o número de ataques virtuais cresceu 10% no Brasil em relação a 2015. No mesmo ano, um total de 42,4 milhões de pessoas no Brasil foram afetadas pelo cibercrime no país, o que representa 39% do total de internautas nacionais.

Entretanto, o ordenamento jurídico brasileiro, carece de leis que regulem de forma eficaz as questões envolvendo proteção de dados pessoais, cibercrimes e demandas gerais sobre segurança na internet. Diante esta asseveração, é possível considerar que existe um grande atraso legislativo combinado com uma falta de interesse dos legisladores pátrios em resolver tais questões. Sendo assim, segundo Almeida (2015, p. 236), o Brasil está em uma situação delicada perante a comunidade internacional, pelo fato de que, “apesar

de ter forte inclusão digital, a contrassenso carece de normas eficazes que regulem as demandas envolvendo a rede mundial de computadores".

Nota-se, desta maneira, que a tarefa de legislar sobre um plano pouco conhecido e que envolve tecnologia de ponta e soberanias estatais é tarefa extremamente complexa, isto é, existem muitas variáveis a serem observadas, lacunas técnicas que devem ser preenchidas e interesses dos mais diversos setores da sociedade que devem ser contrapostos.

Pondera-se que a as duas principais leis brasileiras (lei nº12.737/12 e lei nº12.965/14) que regulam o assunto foram frutos de acontecimentos casuísticos, isto é, sem ter tido um debate adequado acerca da temática. Dessa forma, tem-se a elaboração de leis frágeis, ineficazes e repletas de lacunas jurídicas e técnicas que propiciam a insegurança jurídica. (MARTINS, 2017)

Por conseguinte, a preocupação foi de criar uma legislação que punisse os velhos e novos crimes praticados na internet, fossem eles crimes impróprios ou próprios. Porém, logo se percebeu que seria necessária uma legislação que regulasse condutas, civilmente, antes mesmo que fosse possível puni-las. Em 2014 o Marco Civil da Internet foi um instrumento importante para avanços nessa área, porém, a deficiência legislativa na tipificação de delitos virtuais possui um caminho a percorrer. Neste sentido corrobora (NUNZI, 2012, p. 4):

> As ameaças à segurança em nossas sociedades estão crescendo em escala e sofisticação e o desafio que representam é cada vez mais transfronteiriço e intersetorial. O crime cibernético, que ocupa um lugar de destaque entre as preocupações dos cidadãos e dos governos, corresponde perfeitamente a este perfil, uma vez que se baseia e visa as infraestruturas da Internet e seus usuários. Cidadãos, empresas, governos e infraestruturas críticas precisam de proteção contra os criminosos que exploram as tecnologias modernas.

De acordo com Castells (2009, p. 40), deve-se dar ênfase que "soluções isoladas não conseguem eficácia no plano do ciberespaço, sendo necessárias medidas de atuação regionalizadas objetivando a harmonização legislativa respeitando as diferenças jurídicas e tecnológicas entre os países". Nesta atuação, portanto, especialistas sustentam que tratados ou convenções internacionais poderiam solucionar o problema, tendo em vista que sendo a Internet um meio de comunicação que ultrapassa limites e fronteiras de qualquer país, seria pouco provável que somente leis nacionais de cada Estado

conseguissem definir como, quando, onde e qual legislação seria responsável por determinada conduta delituosa de um indivíduo. (DIAS, 2018, p.56)

Ao analisar esta questão, nota-se a complexidade da extraterritorialidade e a internet nas palavras de (CIDRÃO et. al., 2018, p.69/70):

> Isso faz com que as questões que envolvem a internet sejam de alta complexidade, devido ao fato de estarem relacionadas a várias jurisdições distintas, afetando diferentes países, o que dificulta o entendimento de qual o país seria realmente competente para processar, julgar e penalizar esses infratores cibernéticos. Com efeito, a colisão entre o Direito pátrio e o Direito alienígena quanto à questão do mau uso da Internet faz crer que, para a solução desses conflitos, há a necessidade de se socorrer ao Direito Internacional por meio de acordo de cooperação e tratados. É nesse cenário que os tratados internacionais se fazem um importante instrumento para o combate aos cibercrimes.

Outrossim, conforme Pinheiro (2011), frente as legislações de alcance universal, como a exemplo da Convenção de Budapeste sobre Cibercrimes é um dos melhores instrumentos em busca de uma tutela eficaz, posto que uniformiza o direito material e processual penal nos países membros. Neste sentido, com a Convenção de Budapeste o Estado não desaparece, porém é apenas redimensionado na Era da informação. Tal acordo parte da premissa de que o combate ao cibercrime deve ser realizado através de um Regime Internacional. Noutro giro, a referida Convenção tem objetivos bem demarcados como leciona Boiteux (2004, p. 170).

> harmonizar as legislações penais substantivas, elementos do delito e outras provisões conexas sobre delitos de informática; promover alterações nas legislações processuais nacionais de forma a conceder poderes de investigação e persecução criminais necessários para combater delitos praticados com o uso de sistemas de computador, ou nos demais tipos de delitos nos quais as provas devam ser obtidas mediante meios eletrônicos e estabelecer um regime rápido e efetivo de cooperação internacional.

Nestes moldes, Com relação ao direito material a mencionada Convenção definiu e tipificou os cibercrimes quanto ao acesso e interceptação ilegítima, bem como, interferência de dados e de sistema, uso abusivo de dispositivos, falsidade informática, fraude informática, como também a pornografia infantil virtual e violação de direitos autorais .Todos os crimes definidos na referida Convenção são dolosos, ou seja, “não se admite a possibilidade de conduta delituosa

perpetrada por meio de computador sem que tenha havido a verdadeira intenção de fazê-la". (BOITEUX, 2004, p. 171).

É elementar constatar que, a adesão do Brasil à Convenção de Budapeste não ocorreu logo após o convite formal feito pelo Conselho da Europa. Pelo contrário, demorou alguns anos para isso realmente acontecer. Porém esse foi o primeiro passo para o Estado tomar as providências legais internas necessárias. Nesta perspectiva, cumpra-se salientar que o Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram a tal instrumento internacional multilateral, fortalecendo, assim, os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos. O Decreto nº 11.491, que traz a decisão, foi publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023. (BRASIL, 2023)

Não obstante, além do aperfeiçoamento da cooperação internacional na instrução e elucidação dos delitos praticados no ambiente virtual, a Convenção também impulsiona o Brasil a dar continuidade ao desenvolvimento de seu ordenamento jurídico e de sua política diante do avanço da criminalidade no ambiente cibernético, assim o fazendo com o devido equilíbrio entre a intensificação da persecução penal e a proteção de dados pessoais. Reitera-se, contudo, que o Brasil foi convidado a aderir à Convenção em dezembro de 2019. Pondera-se que o governo federal considera que, embora o Marco Civil da Internet (Lei 12.965, de 2014) tenha criado importante estrutura legislativa para o combate aos crimes cibernéticos, os meios digitais não respeitam fronteiras. Por isso é necessário constante aprimoramento da cooperação e coordenação entre os países. (AGÊNCIA SENADO,2023)

De algum modo, a vida em rede e internet alteram substancialmente as noções de hierarquia, privacidade, cidadania, consumo, bem como da própria democracia, o que encontra espaço de discussão e análise no próprio direito constitucional/eleitoral. Esses aspectos adquirem ainda mais densidade com a disseminação do depeefake, abaixo descrito:

> "o que as redes podem nos proporcionar hoje é a criação de uma nova concepção de democracia, ou de política, que passe da democracia opinativa, representativa, para uma forma mais complexa. (...) Agora, estamos perante a necessidade de um novo tipo de Iluminismo – talvez seja melhor não usar essa designação –, de um novo tipo de transformação que desloque a sensibilidade, o significado mesmo da ação política para além da dimensão exclusivamente humana de

> democracia representativa e para aquém da forma representativa através da qual são tomadas as decisões.” (LEMES, 2014, pag.7)

Pondera-se, no que tangeria à modificação da legislação nacional, tal Convenção dispõe de alguns roteiros que têm como objetivo maior fazer com que os países signatários se comprometam a adotá-los em seus sistemas jurídicos, não sendo exigido, entretanto, que estes venham a copiá-los podendo somente utilizar definições equivalentes. Conforme leciona Boiteux (2004, p. 170) “a Convenção de Budapeste é atualmente o único instrumento jurídico de caráter global para o combate hábil aos cibercrimes”.

Observa-se, além disso, que é preciso acompanhar o tema com atenção para observar e filtrar medidas legislativas e técnicas adotadas por outros países que foram eficazes no combate do uso ilícito dos deepfakes no processo eleitoral e na sociedade como um todo com o objetivo de evitar que os prejuízos advindos dessas condutas tenham influência nas eleições vindouras e em qualquer outra interação social.

Nesse aspecto, é importante salientar que, dentro de uma ordem natural, o direito e, por consequência, as mudanças legislativas, acompanham as mudanças externas, as quais, com o avançar da tecnologia, se propagam rapidamente e se inserem no cotidiano de indivíduos no mundo afora, “cabendo aos legisladores entenderem as novas tendências e proporem redações de novas normativas e adaptações das existentes”. (CASTELLS, 2007, p. 205)

Constata-se, por esse motivo, que a importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados pela Internet, sejam eles tradicionais ou não, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que as leis nacionais têm sua aplicação limitada a um território específico e são totalmente ineficientes no que tange à violação aos direitos humanos e às liberdades individuais.

Em consonância ao delineado, de acordo com Almeida (2015, p. 236): “somente um instrumento internacional poderia ter eficácia na luta contra estes crimes”. Nesta perspectiva, a Cooperação Jurídica Internacional é um instrumento auxiliador dos Estados para assegurar o funcionamento da Justiça em seus territórios, “por meio da qual um Estado, para fins de procedimento no âmbito da sua jurisdição, solicita a outro Estado medidas administrativas ou

judiciais que tenham caráter judicial em pelo menos um desses Estados.” (BRASIL, 2014, p. 78). Esse instituto está, inclusive, previsto na Constituição Federal, no seu artigo 4º, inciso IX, que prevê a “cooperação entre os povos para o progresso da humanidade”. (BRASIL,1988)

Outrossim, é consentâneo indicar que não se trata de uma mera ajuda voluntária ou compromisso moral, mas sim, de uma obrigação jurídica. Assim sendo, além da compatibilidade entre o ordenamento brasileiro e a referida convenção, a escassez de leis específicas sobre o tema dentro do Brasil tem dificultado a aplicação da justiça nos casos concretos. Noutro giro, é elementar considerar que, por ser, de fato, uma obrigação jurídica, não há razão para se sustentar que a cooperação internacional enfraquece a soberania de um país.

Cumpre destacar que a relativização da soberania estatal não está relacionada ao enfraquecimento do Estado diante demais países, mas, pelo contrário, a cooperação internacional está ligada, na verdade, ao papel de cumprimento de obrigações por parte do Estado com seus nacionais e demais países. Ademais, é imprescindível assinalar que a ofensa à soberania, portanto, não pode ser usada como justificativa de um país para cometer violações de direitos e deveres dentro do seu território (FERNANDES,2013).

Dessa forma, a adesão do Brasil à Convenção melhoraria sobremaneira o arcabouço legal do país, permitindo a aprovação de tipos penais específicos, preenchendo importantes lacunas da legislação brasileira que têm prejudicado a efetiva persecução dos crimes cibernéticos. Ademais, a harmonização da legislação nacional com a legislação internacional facilitará a cooperação jurídica internacional em investigações e extradição dos envolvidos.

Além disso, quanto à obtenção de provas, a Convenção possibilitará a cooperação do Brasil com todos os países signatários, inclusive aqueles com os quais não possui acordos bilaterais de cooperação em matéria penal. Deve-se considerar também que de segundo Fernandes (2013, p. 35): “a proteção de dados também será favorecida, eis que a Convenção permite a capacitação e aprimoramento dos investigadores por meio da troca de experiências”. Tão logo, observa-se, que a adesão à Convenção de Budapeste representa um grande avanço na repressão dos crimes cibernéticos, uma vez que proporciona diretrizes fundamentais e soluções para uma tão recente e complexa modalidade criminosa.

Desta forma, contempla-se a aplicabilidade da Convenção de Budapeste ao ordenamento jurídico brasileiro ao combate do *depeefake* com o Decreto nº 11.491 de 12 de abril de 2023, sendo que é preciso impor limites legais dentro de um regime de direito internacional no ciberespaço para que se evitem dilemas jurisdicionais, pois os Estados não podem tratar do assunto individualmente e necessitam buscar, de modo contínuo, a cooperação transnacional ou global para combater eficazmente o crime cibernético.

Nestes moldes, a importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados através da internet, sejam eles puros ou impuros, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que a aplicação de leis internas sobre o referido tema ficaria limitada a somente um território específico e seriam totalmente ineficientes no que diz respeito à violação aos direitos humanos e às liberdades individuais, o que demonstra a inovação da temática e a real importância de se discutir o presente assunto.

CONSIDERAÇÕES FINAIS

O presente trabalho teve por escopo a análise de um dos maiores desafios tecnológicos enfrentados pela sociedade contemporânea, o mal uso dos deep fakes no processo eleitoral e as principais legislações brasileiras que versem sobre a temática. Deste modo, os deepfakes é uma tecnologia relativamente recente, mas que já teve seu potencial criminoso suficientemente demonstrado já em seu surgimento. A atuação do *deepfeke* no Ciberespaço clama por uma regulamentação legal específica que garanta a segurança do que é divulgado à sociedade por meio da internet, que é uma ferramenta usual presente no cotidiano da comunidade mundial, dir-se-ia até mesmo indispensável na contemporaneidade.

Pode-se afirmar que o Brasil, apesar de seu esforço na criação de leis que auxiliem na segurança virtual de seus nacionais, como o Marco Civil da Internet, a Lei Geral de Proteção de dados e as novas leis que preveem as mais recorrentes condutas delitivas no ciberespaço, ainda assim, não dispõe de meios suficientes para coibir de forma eficaz a prática de crimes informáticos, por diversos fatores, como ausência de criminalização de alguns ataques

cibernéticos considerados importantes, por carência da estrutura tecnológica da polícia judiciária para realizar investigações ou, ainda, pela morosidade da Justiça.

Outrossim, sobretudo em matéria eleitoral, entende-se que para que haja ferramentas jurídicas ou tecnológicas hábeis a combater *deepfake* e os demais formatos de notícias fraudulentas, é indispensável a adequação de métodos já existentes em outros países à realidade de nosso cenário interno. Tão logo, a exemplo está a adesão do Brasil à Convenção de Budapeste que ocorreu em 12 de abril de 2023 com Decreto nº 11.491, uma conquista significativa para o país na luta contra crimes cibernéticos. A convenção estabelece normas para prevenção, investigação, detecção e punição desses crimes e permite que países signatários troquem informações de forma mais eficiente.

Nesse sentido, conclui-se, que a convenção incentiva a cooperação internacional e a proteção de dados pessoais dos usuários da internet, isto é, a adesão do Brasil significa que o país se compromete a adotar medidas para prevenir e combater crimes cibernéticos, fortalecer instituições e cooperar internacionalmente. Por essa razão, a adesão do Brasil à Convenção de Budapeste foi um evento tão importante na evolução do ordenamento jurídico nacional, em relação ao combate dos crimes cibernéticos.

Outrossim, foi possível concluir que, que o Brasil tem capacidade e disposição para reprimir a delinquência cibernética. Percebe-se, nos últimos anos, um grande avanço no arcabouço legislativo interno de preocupação com a segurança virtual, e que após adesão da Convenção de Budapeste em seu ordenamento, tornou-se apto para enfrentar essa chaga social denominada: Depeefake.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Jéssica de Jesus. **Crimes cibernéticos**. Periódicos Grupo Tiradentes, v. 2, n.3. p. 215- 236, 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acesso em: 12 de junho 2023

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet.** Rio de Janeiro: Editora Brasport, 2016.

BENKLER, Yochai. **The wealth of networks: how social production transforms markets and freedom.** New Haven: Yale University Press, 2006.

BRANT, Cássio Augusto Barros. **Marco Civil da Internet: Comentários sobre a lei 12.965/2014**. Belo Horizonte: D'Plácido, 2014.

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: 01 de maio de 2023

BRASIL. Ministério da Justiça. **Cartilha de Cooperação Jurídica Internacional em Matéria Penal**. Brasília, DF: Ministério da Justiça, 2014. Disponível em: https://www.justica.gov.br/suaprotecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf. Acesso em: 03 de abril de 2023

BRASIL. Lei nº 12965, de 10 de janeiro de 2002. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União, Brasília, DF, p. 1-11, 23 abr. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm. Acesso em: 09 de maio de 2023

BRASIL. Senado Federal. **Projeto de Lei nº 3.683, de 07 de julho de 2020. Altera a legislação criminal, eleitoral e de improbidade administrativa para elevar penas e sanções de crimes já tipificados e outras condutas ilegais, e criar tipos penais, especialmente quando praticados na internet**. Brasília: Senado federal, 2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8861739&ts=1644253833773&disposition=inline. Acesso em: 10 de maio de 2023

BRASIL. Tribunal Regional Eleitoral de São Paulo, Rec.-RP 7934-2019

BRASIL. Tribunal Regional Eleitoral do Distrito Federal, RP 1764, Rel. Des

.

BRASIL. Tribunal Regional Eleitoral do Distrito Federal, **RRP 275984**, Rel.

BRASIL. Tribunal Superior Eleitoral. **RP 1.402**, Rel. Min. Felix Fischer, DJe

BRASIL. Tribunal Superior Eleitoral. **RP 1.402**, Rel. Min. Felix Fischer, DJe

BRASIL. Tribunal Superior Eleitoral., **Representação 242460**, Min. Henrique Neves da Silva, j. 31.08.2010

CASTELLS, Manuel. **O poder da identidade.** Trad. Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 2018.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2 ed. Rio de Janeiro: Lumen Juris, 2003.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. **A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da convenção de Budapeste à legislação brasileira**.Brazilian Journal of International Relations, Marília, v. 7, n. 1, p. 66-82, jan./abr. 2018.

CITRON, Danielle; CHESNEY, Bobby. **Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.** California Law Review, v. 107, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954. Acesso em: 14 de maio de 2023.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.
DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando da. **Bots, fake news, fake faces, deep fakes e sua eventual influência no processo eleitoral democrático**. In: Revista da Advocacia do Poder Legislativo, v. 2, ano 2021, p. 39.

DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando da. Op. cit., p. 37.
Fabio Assolini. **Deepfake preocupa especialistas, que veem tecnologia incipiente no jogo eleitoral do Brasil**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/deepfake-preocupa-especialistas-que-veem-tecnologia-incipiente-no-jogo-eleitoral-do-brasil/. Acesso em: 15 de maio de 2023

FERNANDES, David Augusto. **Crimes cibernéticos: o descompasso do estado e a realidade.** REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

FERREIRA, Érika Lourenço de Lima. **Internet Macrocriminalidade e Competência Internacional**. Érika Lourenço de Lima Ferreira. 1 edição (ano 2007). Curitiba: Juruá, 2015.

FILIMOWICZ, Michael. **Deep fakes: algorithms and Society**. Nova Iorque: Routledge Focus, 2022

FURQUIM. André Zaca. **Convenção de Budapeste é promulgada no Brasil.** Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 12 de maio de 2023

GOMES, José Jairo. **Direito Eleitoral**, 14ª. ed. rev., atual. (e-book). São Paulo: Atlas, 2018. P. 500.

GOMES, Luiz Flávio. **Lei "Carolina Dieckmann" e sua (in)eficácia.** Jus Navigandi, Teresina, ano 18, nº 3.536, Disponível em: <http://jus.com.br/revista/texto/23897>. Acesso em: 04 de abril de 2023.

HERMANN, Nadja. **Ética & educação: outra sensibilidade.** Belo Horizonte: Autêntica, 2014. Coleção Temas & Educação

HOFMANN, Jeanette. **Mediated democracy – Linking digital technology to political agency**. Internet Policy Review, v. 8, n. 2, 30 jun. 2019 João Mariosi, DJe 29.10.2009.

JUSTIÇA ELEITORAL. **Fato ou Boato**. Brasil: JUSTIÇA ELEITORAL, 2022. Disponível em: https://www.justicaeleitoral.jus.br/fato-ou-boato/. Acesso em:
LEAL, Luziane de Figueiredo Simão. Inteligência Artificial nas campanhas eleitorais: a democracia das plataformas no banco dos réus. Belo Horizonte: Dialética, 2020. P. 72-73.

LEMOS, Ronaldo; FELICE, Massimo di. **A Vida em Rede**. Campinas: Papirus 7 Mares, 2014

LIRA. Leide de Almeida. **Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Brasília. 2014. Disponível em: www.conteudo jurídico.com.br. Acesso em: 10 de maio de 2023

MARTINS, AISLAN**. Crimes Virtuais**. Sabará 2017. Disponível em: <https://www.faculdadesabara.com.br/media/attachments/monografias/Monografia_CrimesVirtuais_Aluno-Aislan.pdf>

MOLINA, AC; BERENGUEL, OL **Deepfake: a evolução das notícias falsas. Investigação, Sociedade e Desenvolvimento**., v. 11, n. 6, pág. e56211629533, 2022. DOI: 10.33448/rsd-v11i6.29533. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/29533. Acesso em: 14 maio. 2023.

MOURA, Maurício. **Seminário Internacional Fake News e Eleições** [recurso eletrônico]: anais. Brasília: Tribunal Superior Eleitoral, 2019. 58. Acesso em: 17 de abril de 2023.

NEVES, Barbara. **Recursos que podem apoiar o bibliotecário no combate às Fake News nas mídias sociais.** v. 8, p. 17-27, 2019. Disponível em:

https://revistas.ufpr.br/atoz/article/view/68094/41066. Acesso em: 09 de junho de 2023.

NEVES, F.F; VANCIM A.R. **Marco Civil da Internet** – Anotações à Lei nº anotações à Lei nº 12.965/2014.

PECK, Patricia. **Peck: Sobre a adesão do Brasil à Convenção de Budapeste**. Disponível em: https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/. Acesso em: 05 de maio de 2023

PINHEIRO, Patrícia Peck. **Direito digital.** 4. ed. Revista, atualizada e ampliada. São Paulo: Saraiva, 2ª tiragem 2011.

RECUERO, Raquel**. Redes sociais na Internet**. Porto Alegre: Sulina, 2009.
RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUEDIGER, Marco Aurélio (coord.). **Bots e o Direito Eleitoral brasileiro nas eleições de 2018.** Rio de Janeiro: FGV DAPP, 2018. P. 5. Disponível em: <http://twixar.me/DmNT>. Acesso em: 24 de maio de 2023.

SOLOVE, Daniel. J. **The future of reputation: gossip, rumor, and privacy on the Internet**. New Haven: Yale Univ. Press, 2007

SPENCER, Michael K. **Deep Fake, a mais recente ameaça distópica**. Outras Palavras, 30 maio 2019. Disponível em: outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia. Acesso em: 15 de maio de 2023

VOGT, Jackson**. Direito Cibernético: análise da legislação penal e a Convenção de Budapeste.** Disponível em: < https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/1531>. Acesso em: 20 de maio de 2023

WESTERLUND, Mika. **The emergence of deep fake technology: a review. In: Technology Innovation Management Review**. v. 9, nº 11, nov. 2019. Disponível em: <https://timreview.ca/article/1282> Acesso em: 07 de abril de 2023.

YOUNG, Norbet. **DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media.** 2019. Edição Kindle, 160p.