

CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO EM DIREITO

FÁBIO LEANDRO MELO RAMOS DOS ANJOS

MARIA BRENDA NUNES DE BARROS

***Deepfakes* e os desafios jurídicos na era Digital no Brasil**

RECIFE/2025

FÁBIO LEANDRO MELO RAMOS DOS ANJOS
MARIA BRENDA NUNES DE BARROS

***Deepfakes* e os desafios jurídicos na era Digital no Brasil**

Trabalho de conclusão de curso
apresentado à Disciplina TCC II do
Curso de Bacharelado em Direito do
Centro Universitário Brasileiro -
UNIBRA, como parte dos requisitos
para conclusão do curso.

Orientador(a): Prof. Esp. Marisol
Tatiane Teixeira Bezerra

RECIFE/2025

Folha reservada para Ficha Catalográfica

FÁBIO LEANDRO MELO RAMOS DOS ANJOS
MARIA BRENDA NUNES DE BARROS

***Deepfakes* e os desafios jurídicos na era Digital no Brasil**

Trabalho de conclusão de curso apresentado à Disciplina TCC II do Curso de Direito do Centro
Universitário Brasileiro - UNIBRA, como parte dos requisitos para conclusão do curso.

Examinadores:

Orientador – Marisol Tatiane Teixeira Bezerra

Examinador 1 - Titulação

Examinador 2 - Titulação

Nota: _____

Data: __/__/____

RESUMO

O projeto em questão buscou investigar os desafios jurídicos impostos pelo uso de *deepfakes* na era digital, com foco na realidade brasileira. Parte-se da questão central: como a legislação brasileira pode enfrentar os riscos e lacunas decorrentes do uso de *deepfakes*? Para responder a esse problema, o objetivo geral consiste em apresentar uma análise crítica das lacunas na legislação brasileira e dos desafios jurídicos enfrentados em relação às manipulações audiovisuais, com ênfase na criação de propostas para adaptação da legislação às novas realidades digitais. A relevância do estudo reside na crescente disseminação de *deepfakes*, que potencializa práticas de desinformação, fraude e violações de direitos individuais e coletivos, colocando em risco a segurança jurídica e a confiança nas comunicações eletrônicas. A metodologia adotada é qualitativa, com fundamentação teórica e revisão bibliográfica de doutrinas, artigos acadêmicos e legislações comparadas, além da análise de casos concretos e de boas práticas regulatórias, sobretudo na União Europeia. Espera-se, como resultados parciais, mapear as principais falhas na legislação brasileira, como a inexistência de tipificação específica de *deepfakes* e a carência de mecanismos eficazes de detecção e responsabilização, além de compilar soluções adotadas em outros países que possam servir de referência. Como produtos finais, serão apresentadas recomendações de atualizações do ordenamento jurídico brasileiro, bem como diretrizes para cooperação público-privada e utilização de tecnologias de detecção automatizada. Antecipam-se, por fim, contribuições que ofereçam possibilidades regulatórias para a sociedade de forma flexível e abrangente, capaz de preservar direitos fundamentais e aprimorar a resposta do sistema de justiça aos impactos das inovações tecnológicas.

Palavras-Chaves: *Deepfakes*, Direito Digital, Evolução, Legislação, Regulamentação.

Deepfakes and Legal Challenges in the Digital Age in Brazil

ABSTRACT

The project in question sought to investigate the legal challenges posed by the use of deepfakes in the digital age, with a focus on the Brazilian reality. The central question is: how can Brazilian legislation address the risks and gaps arising from the use of deepfakes? To answer this problem, the general objective is to present a critical analysis of the gaps in Brazilian legislation and the legal challenges faced in relation to audiovisual manipulations, with an emphasis on creating proposals for adapting legislation to the new digital realities. The relevance of the study lies in the growing dissemination of deepfakes, which enhances practices of disinformation, fraud and violations of individual and collective rights, putting legal security and trust in electronic communications at risk. The methodology adopted is qualitative, with a theoretical foundation and bibliographic review of doctrines, academic articles and comparative legislation, as well as an analysis of concrete cases and good regulatory practices, especially in the European Union. Partial results are expected to include mapping the main flaws in Brazilian legislation, such as the lack of a specific definition of deepfakes and the lack of effective detection and accountability mechanisms, as well as compiling solutions adopted in other countries that can serve as a reference. The final product will be recommendations for updating the Brazilian legal system, as well as guidelines for public-private cooperation and the use of automated detection technologies. Finally, contributions are anticipated that offer regulatory possibilities for society in a flexible and comprehensive way, capable of preserving fundamental rights and improving the justice system's response to the impacts of technological innovations.

Keywords: *Deepfakes*, Digital Law, Evolution, Legislation, Regulation.

SUMÁRIO

1. Introdução.....	6
2. Origem e Evolução dos <i>Deepfakes</i>: do Potencial Inovador aos Riscos Jurídicos.....	7
3. Legislação Brasileira: Desafios para o Enfrentamento dos <i>Deepfakes</i>.....	9
4. Comparação com a Legislação Europeia: o Caso de Portugal como Referência.....	11
5. Possibilidades para o Aprimoramento da Legislação sobre os <i>Deepfakes</i>.....	12
5.1 Desenvolvimento de uma Legislação Específica para <i>Deepfakes</i>	12
5.2 Atualização e Reforço das Normas Existentes.....	14
5.3 Implementação de Tecnologias de Detecção.....	15
5.4 Tribunal Superior Eleitoral: Iniciativa Pioneira na Regulação de <i>Deepfakes</i>	15
5.5 A Lei nº 15.123/2025 e o Reconhecimento dos <i>Deepfakes</i> como Forma de Violência Psicológica contra a Mulher.....	17
6. Conclusão.....	17
7. Referências.....	18

1. Introdução

A evolução digital tem transformado profundamente diversas esferas da sociedade, incluindo o campo jurídico. Entre as inovações tecnológicas que trazem novos desafios para o direito, os *deepfakes* se destacam como uma questão particularmente complexa e relevante. Esta Inteligência Artificial (IA) utiliza técnicas avançadas para criar representações falsas e realistas de vídeos e áudios, cada vez mais inovadores e acessíveis. A tecnologia tem o potencial de gerar consequências significativas, como a disseminação de desinformação, criação de fraudes e violação de privacidade, afetando tanto o meio empresarial quanto o pessoal, e colocando em dúvida a credibilidade de pessoas e instituições.

No contexto brasileiro, a legislação atual enfrenta dificuldades para lidar com as implicações jurídicas dos *deepfakes*, uma vez que a tecnologia evolui rapidamente, enquanto as normas legais ficam defasadas. Este projeto de pesquisa teve como objetivo geral apresentar uma análise crítica das lacunas na legislação brasileira e dos desafios jurídicos enfrentados em relação às manipulações audiovisuais, com ênfase na criação de propostas para adaptação da legislação às novas realidades digitais. Para alcançar este objetivo, foram abordados três objetivos específicos: (i) investigar as características técnicas dos *deepfakes* e suas implicações jurídicas; (ii) examinar as lacunas legislativas e seus efeitos jurídicos em relação aos *deepfakes*; e (iii) avaliar o avanço da legislação brasileira na proteção contra os efeitos dos *deepfakes*. Através do resultado desta investigação, pretende-se contribuir para um entendimento mais profundo dos desafios que essa forma de inteligência artificial representa para o direito e para a construção de soluções que possam alinhar a legislação brasileira às novas realidades digitais.

A rápida evolução das tecnologias digitais, como os *deepfakes*, tem gerado uma série de desafios para o direito, especialmente em relação à proteção dos direitos fundamentais e à manutenção da ordem social. Diante desse cenário, a questão central deste estudo foi: “Como a legislação brasileira pode enfrentar os desafios jurídicos decorrentes do uso de *deepfakes*?”.

A hipótese desta pesquisa é que a legislação brasileira, na sua forma atual, enfrenta dificuldades para lidar com os desafios impostos pelos *deepfakes*, resultando em lacunas significativas na proteção dos direitos fundamentais e na manutenção da ordem social. A rápida evolução das tecnologias de manipulação audiovisual e a defasagem das normas legais existentes criam a possibilidade de que as respostas jurídicas atuais sejam insuficientes para lidar com estas implicações. Sendo necessário, portanto, desenvolver propostas legislativas e regulatórias que estejam alinhadas com as novas realidades digitais, garantindo uma proteção jurídica adequada contra as consequências prejudiciais das manipulações digitais.

O estudo se justifica pela crescente relevância dessa tecnologia na sociedade e pelas implicações legais ainda não totalmente exploradas. O avanço tecnológico, especialmente em inteligência artificial, trouxe à tona novas questões, exigindo uma reavaliação das normas para garantir a proteção adequada dos indivíduos e das instituições. *Deepfakes*, caracterizados pela manipulação digital de vídeos e áudios para criar representações falsas, têm o potencial de causar danos relevantes, como a já mencionado, desinformação, fraudes e violações. Esses riscos são agravados pela acessibilidade crescente dessas tecnologias, o que torna sua regulação um desafio complexo.

A utilização indevida de *deepfakes* pode ser definida como ato ilícito, já que pode violar direitos individuais, como a imagem e a honra, gerando danos morais. De acordo com o artigo 186 do Código Civil¹, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” (BRASIL, 2002). Além disso, o artigo 927 complementa, estabelecendo que “aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo” (BRASIL, 2002). Com isso, a criação e disseminação de *deepfakes* que causem prejuízo moral ou material gera a responsabilidade de reparação do dano.

No Brasil, a legislação atual enfrenta dificuldades para acompanhar a rápida evolução da inteligência artificial, especificamente os *deepfakes*, o que resulta em uma lacuna normativa preocupante. A ausência de regulamentação específica para essas tecnologias coloca em risco a segurança jurídica e a proteção dos direitos fundamentais, como a privacidade, a honra e a imagem das pessoas. Além disso, a utilização maliciosa desse tipo de tecnologia pode minar a confiança pública nas mídias digitais e comprometer a

¹ BRASIL. **Código Civil**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 27/04/2025.

integridade das informações veiculadas.

Esta pesquisa visou compreender como o direito brasileiro pode evoluir para lidar com essa problemática. A análise crítica das lacunas na legislação vigente e a proposição de soluções jurídicas inovadoras são essenciais para garantir que o ordenamento jurídico esteja preparado para proteger os cidadãos e manter a ordem social na era digital. Este estudo possibilitará uma contribuição para o desenvolvimento de uma base legal que possa responder adequadamente às novas realidades tecnológicas, promovendo a justiça e a segurança no âmbito digital.

O caminho metodológico traçado para o desenvolvimento deste projeto utilizou uma abordagem qualitativa, teórica e revisão bibliográfica de autores de referência e doutrinas nacionais e internacionais. A pesquisa envolveu um método detalhado dos aspectos legais e tecnológicos relacionados aos *deepfakes*. Para isso, foram analisados livros e artigos de direito e segurança digital, além de observação de casos práticos envolvendo *deepfakes* e legislação.

O projeto incluiu uma análise cuidadosa das dificuldades enfrentadas pelo sistema jurídico brasileiro em lidar com *deepfakes*, utilizando como referência obras de autores como Pinheiro² Prado³ e Teixeira⁴, que oferecem uma base teórica relevante para o tema. Adicionalmente, a pesquisa bibliográfica foi enriquecida com a contribuição dos autores Assad, Bignoto, Lima, Neto e Vieira⁵, conforme citação a seguir:

A pesquisa bibliográfica é aquela elaborada a partir de material já publicado, como livros, artigos de periódicos, dicionários, enciclopédias, impressos diversos, publicações periódicas, revistas e jornais e de material disponibilizado na internet. A pesquisa bibliográfica permite ao pesquisador a cobertura de uma gama de fenômenos muito ampla, principalmente quando o problema a ser investigado necessita de informações muito dispersas. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica (referimo-nos ao estudo do tema com base na literatura disponível), que permite ao pesquisador conhecer o que já se estudou sobre o assunto.

Assim, os autores explicam que a pesquisa bibliográfica envolve o estudo das principais obras, como artigos científicos, leis e livros na área de interesse. Essa abordagem foi crucial, pois proporcionou acesso as informações atuais e essenciais reunidas em uma única fonte sobre o tema. Esse tipo de pesquisa possibilita uma nova perspectiva, permitindo que o leitor obtenha uma visão mais abrangente e ajude na compreensão e desenvolvimento de novas ideias e soluções inovadoras relacionadas ao assunto.

2. Origem e Evolução dos *Deepfakes*: do Potencial Inovador aos Riscos Jurídicos

Os *deepfakes* surgiram no final da década de 2010 nos EUA, impulsionados pelos avanços na inteligência artificial e no aprendizado profundo (*deep learning*). O termo "*deepfakes*" é uma combinação de "*deep learning*" e "*fake*", refletindo a natureza da tecnologia que utiliza redes neurais artificiais para manipular vídeos e áudios de forma extremamente realista. Prado⁶ descreve em sua obra, como surgiu a tecnologia:

Em dezembro de 2017, um usuário do Reddit utilizando ferramentas de Inteligência Artificial e Aprendizado de Máquina de código aberto, como o Keras e o TensorFlow (esse último, do Google), criou um algoritmo para treinar uma rede neural a mapear o rosto de uma pessoa no corpo de outra,

² PINHEIRO, Patrícia Peck; **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

³ PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse**. TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.

⁴ TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico**. 5. Ed. São Paulo: Saraiva Educação, 2020.

⁵ CHEHUEN Neto, J. A., ASSAD, I. M., BIGNOTO, T. C., LIMA, W. G., & VIEIRA, C. M; **A pesquisa científica e suas classificações**. In J. A. Chehuen Neto (Org.), Metodologia, modelos e estatística aplicados à pesquisa científica na área da saúde (pp. 76–101). Juiz de Fora: Editora UFJF, 2022. Disponível em <https://www2.ufjf.br/editora/wp-content/uploads/sites/113/2022/09/Metodologia-Modelos-e-Estat%C3%ADstica-1.pdf>. Acessado em 07/05/2025.

⁶ PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse**. TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.

frame por frame. Ao invés de usar edição manual como antes, o usuário através da ferramenta (que recebeu o nome de Deep Fake) precisa apenas de uma fonte para reconhecer o modelo do rosto da 'vítima', mapear a estrutura da cabeça-destino e fazer a sobreposição. O software é capaz de ajustar a movimentação do vídeo original ao novo rosto e isso inclui expressões faciais e movimentos labiais." (Gogoni, 2018, apud Prado, 2021, p. 12).

Inicialmente, essa tecnologia foi desenvolvida com finalidades inovadoras, como a criação de efeitos especiais no cinema, a reconstrução de rostos de atores em produções audiovisuais e a dublagem de vozes com alta precisão, permitindo a simulação de figuras públicas em contextos controlados e consentidos. Situação bem diferente da intenção trazida na afirmação de Prado⁷.

Os primeiros usos legítimos de dados manipulados eram vistos como avanços significativos na indústria do entretenimento e no campo da comunicação digital. Por exemplo, eles possibilitam a recriação de personagens históricos em filmes e documentários, ou a substituição de rostos em cenas sem a necessidade de refilmagens, reduzindo custos e ampliando as possibilidades criativas, inclusive em propagandas. Entretanto, com a popularização da tecnologia e a disponibilidade de ferramentas de criação de imagens geradas por IA em plataformas acessíveis, como aplicativos de smartphones e softwares de códigos abertos, os quais qualquer pessoa pode modificar, essa inovação começou a ser explorada para fins maliciosos.

Sobre tal questão, asseveram Alves et al.⁸:

Conforme se observa, a princípio, os fins aos quais os “deep fakes” se destinavam eram completamente lícitos, auxiliando na produção de obras artísticas. Contudo, com o passar do tempo, a tecnologia foi se popularizando e se aperfeiçoando, ganhando espaço na seara humorística, motivo pelo qual começou a ser empregada para satirizar indivíduos e situações.

A utilização de “deep fakes” para a sátira, por si só, já gera questionamentos acerca de sua repercussão jurídica, tendo em vista que, a depender da situação concreta, pode ofender a dignidade das pessoas que aparecem nos vídeos.

Entretanto, com o passar do tempo, os “deep fakes” estão, cada vez mais, sendo utilizados para objetivos inquestionavelmente ilícitos, como a adulteração de vídeos de candidatos, de modo a manipular o resultado de eleições; a inserção do rosto de atrizes em vídeos pornográficos; a criação de perfis falsos para a prática de crimes e a adulteração de meios de prova.

O aspecto mais preocupante da evolução tecnológica da IA é sua capacidade de produzir conteúdo falsos que são quase imperceptíveis de materiais autênticos. Vídeos manipulados podem mostrar indivíduos dizendo ou fazendo coisas que nunca aconteceram, como colocar atrizes de sucesso de filmes tradicionais de romance ou comédia em cenas de plataformas pornográficas. A exemplo disso, faces de alunas da escola do ensino médio na Barra da Tijuca sendo utilizadas para colocar em corpos de atrizes de filme pornográfico além de diversas outras possibilidades mal-intencionadas.

Esse tipo de manipulação, quando envolve crianças ou adolescentes, é tipificado como crime em nosso ordenamento jurídico. Conforme previsto no Estatuto da Criança e do Adolescente⁹:

Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

⁷ PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse**. TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.

⁸ ALVES, Bruno Moraes; ARAÚJO, Ana Karem Vasconcelos; CAVALCANTE, Juan Fonteles; et al. **Análise da responsabilização criminal dos criadores e propagadores de “deep fakes” no ordenamento jurídico brasileiro**. *Caderno Pedagógico*, v. 21, n. 6, p. e4348, 2024. DOI: <https://doi.org/10.54033/cadpedv21n6-075>. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348>. Acesso em 09/05/2025.

⁹ BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18069.htm. Acesso em 08/05/2025.

Tais situações criam um potencial enorme para a disseminação de desinformação, fraudes, campanhas de difamação e outras formas de manipulação social. O uso de *deepfakes* em crimes como extorsão, chantagem e pornografia não consensual tornou-se uma realidade alarmante, colocando em risco a privacidade e a segurança de indivíduos em todo o mundo. Conforme observado por Teixeira¹⁰:

A privacidade é uma questão bastante relevante, tanto que é considerada direito fundamental. Sua violação, inclusive, é vedada pela Constituição Federal de 1988, art. 5º, inc. X. Entretanto, com a chegada da internet, a privacidade pode ter encontrado uma grande vilã nessa avançada rede de comunicação.

Reforçando a ideia de que a privacidade está em risco dentro do contexto jurídico em confronto com as manipulações digitais realistas que apresentam desafios significativos. A facilidade com que esses vídeos podem ser criados e disseminados torna difícil rastrear a origem do conteúdo e identificar os responsáveis pela manipulação. Além disso, a qualidade do resultado da produção de vídeos manipulados pode comprometer a integridade das provas digitais em processos judiciais, dificultando a distinção entre o que é real e o que é fabricado.

Os desafios são intensificados pela ausência de uma regulamentação específica em muitos países, incluindo o Brasil, onde a legislação atual muitas vezes não é capaz de acompanhar a evolução das tecnologias digitais. Pinheiro¹¹ observa que os conteúdos falsos ou manipulados com o objetivo de desinformar vêm ganhando espaço, influenciando diretamente as crenças e opiniões públicas, seja por motivos de manipulação ou financeiros, com base em cliques que geram retornos econômicos.

Praticamente, os *deepfakes* começaram como uma ferramenta inovadora com potencial positivo em diversas indústrias de entretenimento, mas sua melhoria rápida, adaptações e a facilidade do uso, geram consequências de criação ilícita o que leva a uma série de riscos jurídicos e sociais. A necessidade de uma resposta robusta por parte do direito se tornou imperativa e necessária, exigindo não apenas a atualização das leis existentes, mas também a criação de novos mecanismos de proteção e responsabilização que possam lidar com as complexidades introduzidas por essa tecnologia.

3. Legislação Brasileira: Desafios para o Enfrentamento dos *Deepfakes*

A rápida disseminação dos *deepfakes* trouxe à tona desafios legais significativos, que têm revelado a inadequação jurídica brasileira para lidar com as complexidades introduzidas por essa tecnologia. O direito, tradicionalmente fundamentado em conceitos de prova, autenticidade e veracidade, encontra-se diante de uma realidade em que a linha entre o real e o artificial é cada vez mais sutil, criando dificuldades para a aplicação das normas vigentes.

Uma das principais lacunas na legislação brasileira é a ausência de normas específicas que tratam diretamente dos *deepfakes*. Atualmente, os crimes contra a honra cometidos por meio de manipulações audiovisuais, como difamação, injúria, calúnia, falsidade ideológica, ou divulgação de conteúdo íntimo sem consentimento, são definidos em leis que não foram concebidas para lidar com os detalhes dessa tecnologia. Teixeira¹² corrobora em sua obra que

O Código Penal brasileiro prevê os crimes contra a honra nos arts. 138 e s.: calúnia (atribuir falsamente a prática de um crime a alguém inocente), injúria (ofender a dignidade de outra pessoa) e difamação (atribuir fato ofensivo à reputação de outrem), que por sua vez são facilmente praticados pela internet.

Crimes contra a honra, quando são praticados em ambiente virtual, como é a internet, podem provocar às vítimas danos em extensão bem maior do que se praticados nas vias ordinárias da vida real. Isso porque uma informação circulando na rede e/ou colocada em comunidades virtuais (redes sociais) alcança um número ilimitado de pessoas, uma vez que houve uma ampliação do espaço "público" por onde os efeitos do crime poderiam percorrer.

¹⁰ TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico**. 5. Ed. São Paulo: Sairava Educação, 2020.

¹¹ PINHEIRO, Patrícia Peck; **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

¹² TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico**. 5. Ed. São Paulo: Saraiva Educação, 2020.

O Código Penal¹³ brasileiro somado a Lei de Crimes Informáticos¹⁴, conhecida como "Lei Carolina Dieckmann", podem ser utilizados para penalizar a utilização maliciosa de *deepfakes*, mas tais dispositivos legais não abordam diretamente tal situação, deixando margem para interpretações variadas e, muitas vezes, insuficientes. Pinheiro¹⁵ considera que

Dentro da nova realidade da sociedade digital, é fundamental repensar alguns princípios jurídicos, bem como resgatar os valores aos quais tais princípios estão atrelados e que motivaram a existência das leis que se encontram em vigor. É preciso interpretar as normas legais de acordo com as novas situações, que merecem novas respostas.

Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD)¹⁶, embora possa prever proteção de dados pessoais, ela não aborda explicitamente as manipulações de imagem e voz, o que pode resultar em proteção insuficiente ou incerta para as vítimas desse tipo de tecnologia.

Outro desafio é a dificuldade de aplicação das normas existentes no ambiente digital. A identificação dos autores é complexa devido ao anonimato frequentemente proporcionado pela internet e às técnicas de ocultação digital. Teixeira¹⁷ contribui quando explica que conforme a visão clássica do instituto da responsabilidade civil, a culpa do agente era um elemento essencial para que houvesse responsabilização pelo dano causado. Dessa forma, além de provar o nexo causal e o dano sofrido, a vítima também precisava demonstrar a culpa do agente, o que caracterizava a chamada responsabilidade civil subjetiva.

Somado a isso, a natureza internacional da internet permite que os responsáveis por criar e disseminar informações falsas estejam fora da jurisdição brasileira, o que complica ainda mais a aplicação da lei e a responsabilização dos culpados. Hoffmann-Riem¹⁸ em sua obra corrobora com o texto a seguir

como a proteção jurídica individual não é de forma alguma suficiente para afastar os riscos engendrados pela digitalização, também deve ser assegurada a fiscalização pública eficaz do cumprimento dos regulamentos. As instituições criadas até o momento, como os responsáveis pela proteção de dados, não são suficientes para este fim, pelo menos não na medida em que se refere mais do que a proteção de dados pessoais pelos quais são responsáveis.

Diante da insuficiência das instituições atuais para garantir uma fiscalização pública eficaz, conforme destacado na citação anterior, observa-se que essa limitação não afeta apenas a proteção de dados pessoais. A ausência de regulamentação específica tem implicações ainda mais amplas, impactando diretamente a atuação das autoridades judiciais. Desta forma, sem uma base legal clara, o judiciário enfrenta dificuldades para julgar casos envolvendo *deepfakes*, especialmente no que tange à coleta de provas e à autenticação de evidências digitais.

Nesse contexto, é evidente que o Brasil precisa avançar na criação de uma legislação específica que trate dos *deepfakes*, abrangendo tanto a responsabilização dos possibilitadores (plataformas), criadores e disseminadores desse tipo de conteúdo quanto a proteção eficaz das vítimas. O processo legislativo deve considerar as melhores práticas internacionais, adaptar-se às peculiaridades do ambiente digital e ser flexível o suficiente para acompanhar a evolução tecnológica.

Em síntese, as lacunas na legislação brasileira evidenciam a necessidade de uma revisão e atualização das normas jurídicas para enfrentar adequadamente os desafios impostos pela clonagem digital. Sem essa evolução legislativa, o país corre o risco de ficar desprotegido diante de uma tecnologia que tem o potencial de impactar negativamente não apenas na questão da privacidade e reputação individual, mas também na integridade do próprio sistema de justiça.

¹³ BRASIL. **Código Penal**. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

¹⁴ BRASIL. **Lei Nº 12.737, de 30 de Novembro de 2012**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em 07/05/2025.

¹⁵ PINHEIRO, Patrícia Peck; **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

¹⁶ BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 07/05/2025.

¹⁷ TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico**. 5. Ed. São Paulo: Saraiva Educação, 2020.

¹⁸ HOFFMANN-RIEM, Wolfgang; **Teoria Geral do Direito Digital: desafios para o direito**. Rio de Janeiro: Forense, 2021.

4. Comparação com a Legislação Europeia: o Caso de Portugal como Referência

A crescente ameaça representada pelos *deepfakes* tem levado diversos países a repensarem suas abordagens legislativas para garantir a proteção dos cidadãos contra os impactos dessa tecnologia. Entre os países europeus, Portugal, juntamente com a União Europeia, desponta como uma referência no enfrentamento jurídico das produções audiovisuais geradas por IA, destacando-se pela implementação de medidas mais avançadas e específicas em comparação com outras nações, incluindo o Brasil.

Portugal, ao integrar-se ao quadro legislativo da União Europeia, tem se beneficiado de um ambiente jurídico que valoriza a proteção de dados pessoais e a segurança digital. A regulamentação europeia, particularmente o Regulamento Geral de Proteção de Dados¹⁹ (RGPD), estabelece uma base sólida para a proteção contra o uso indevido de tecnologias como os *deepfakes*. O RGPD impõe obrigações rigorosas sobre o tratamento de dados pessoais, o que inclui a imagem e a voz de indivíduos.

No art. 83 da RGPD deixa explícito que dados biométricos são

dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais.

O que significa que a criação e disseminação de *deepfakes* depende do consentimento das pessoas envolvidas, caso contrário podem ser enquadradas como violações graves de privacidade, sujeitas a sanções mais rígidas.

Especificamente em Portugal, a aplicação do RGPD é complementada por uma série de legislações nacionais que abordam questões de cibersegurança e crimes digitais. O Código Penal²⁰ português, por exemplo, em seu artigo 221 (Burla Informática e nas Comunicações) inclui crimes relacionados à manipulação de dados e à disseminação de informações falsas e determina a penalidade de até 3 anos ou multa. Além disso, a República Portuguesa implementou uma estratégia nacional de cibersegurança que enfatiza a proteção contra ameaças digitais emergentes, como os *deepfakes*, e a criação de mecanismos de resposta rápida a incidentes cibernéticos.

Um dos aspectos mais inovadores da legislação portuguesa é a previsão de sanções específicas para a criação e divulgação de conteúdos falsos que visem prejudicar a honra, a dignidade ou a reputação de um indivíduo. Essas disposições oferecem uma proteção mais direta e eficaz, especialmente em casos de uso não consensual de imagem e voz que possam resultar em danos significativos às vítimas. Além do mais, Portugal adota uma abordagem preventiva, incentivando a educação digital e a conscientização pública sobre os riscos associados à criação de conteúdos falsos, promovendo assim uma cultura de responsabilidade e ética no uso de tecnologias digitais.

Em contraste, a legislação brasileira ainda carece de medidas específicas que tratem dos *deepfakes* de forma abrangente. Enquanto em Portugal o ambiente jurídico já incorpora a proteção contra manipulações digitais avançadas, o Brasil ainda depende de legislações mais gerais, como os Códigos Civil²¹ e Penal²² e a Lei Geral de Proteção de Dados²³, que não foram originalmente desenvolvidas para lidar com os desafios que surgem por meio da tecnologia de inteligência artificial. Essa diferença de abordagem nos deixa em desvantagem, especialmente considerando o rápido avanço desse sistema e a crescente sofisticação dos *deepfakes*.

¹⁹PORTUGAL. **Lei N.º 58/2019.** Disponível em https://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=leis&artigo_id=&nid=2961&nversao=&tabela=leis. Acesso em 06/05/2025.

²⁰PORTUGAL. **Decreto-Lei n.º 48/1995.** Aprova o Código Penal. Disponível em: <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675>. Acesso em 06/05/2025.

²¹ BRASIL. **Código Civil.** Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 27/04/2025.

²² BRASIL. **Código Penal.** Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

²³ BRASIL. **Lei N.º 13.709, de 14 de Agosto de 2018.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 07/05/2025.

A experiência do país lusitano serve como um exemplo valioso para o Brasil, destacando a importância de uma legislação adaptada às novas realidades digitais. A integração de medidas específicas, combinada com uma abordagem de cibersegurança abrangente, oferece um modelo eficaz que pode ser seguido para fortalecer a proteção legal contra os riscos associados às manipulações digitais realistas. Adotar uma legislação inspirada nas melhores práticas europeias, como as implementadas em Portugal, pode ser um passo importante para que o Brasil enfrente os desafios de maneira mais robusta e eficaz.

5. Possibilidades para o Aprimoramento da Legislação sobre os *Deepfakes*

A rápida evolução e disseminação das tecnologias de *deepfakes* têm gerado desafios complexos para a legislação brasileira, que ainda enfrenta lacunas expressivas no tratamento desse fenômeno digital. Para enfrentar eficazmente as dificuldades apresentadas e proteger direitos fundamentais, é essencial que o Brasil adote uma abordagem robusta e adaptada às especificidades dessa tecnologia. A seguir, serão apresentadas possibilidades para o fortalecimento da legislação brasileira, com base nas lacunas identificadas e nas práticas internacionais.

5.1 Desenvolvimento de uma Legislação Específica para *Deepfakes*

A criação de um marco legal específico é crucial. Essa legislação deve abranger a definição clara de *deepfakes*, estabelecendo o que caracteriza essa tecnologia e os diferentes tipos de manipulações digitais envolvidas. Além disso, deve prever a criminalização dos usos indevidos, tipificando como crimes a criação e disseminação que causem danos à honra, à privacidade ou à integridade de indivíduos, bem como a desinformação e fraudes. A partir disso, Fidelis e Soares²⁴ destacam a necessidade da criação de técnicas de identificação para enfrentar os desafios impostos

Interessante destacar que, a mesma difusão de técnicas de aprendizagem de máquina na utilização de trocas de faces, em conjunto com a mesma temática discutida acerca da facilidade do acesso às essas ferramenta pelos usuários, possibilitam pesquisadores da área de inteligência artificial, desenvolverem tecnologias capazes de detectar *deepfakes*, e identificar mudanças no futuro que sejam indetectáveis pelos olhos humanos, o que já está ocorrendo.

Nesse contexto, existe o Projeto de Lei (PL) nº 2.338/2023²⁵, de autoria do Senador Rodrigo Pacheco, que busca instituir um marco legal para o uso da inteligência artificial no Brasil. A proposta estabelece princípios, direitos e deveres para o desenvolvimento e a aplicação responsável dessa tecnologia, visando garantir a transparência, a segurança, a proteção de dados e o respeito aos direitos fundamentais. O projeto também aborda a necessidade de mecanismos de governança e supervisão, bem como a previsão de sanções em casos de uso abusivo da IA. Após sua aprovação no Senado, o texto foi remetido à Câmara dos Deputados, onde se encontra em tramitação. Essa iniciativa representa um passo importante para a consolidação de um ambiente regulatório que contemple as especificidades da IA, incluindo as tecnologias de manipulação digital como os *deepfakes*. Ferreira²⁶, corrobora em seu projeto da seguinte forma

a legislação e as políticas digitais podem ser reavaliadas com o objetivo de promover uma sociedade mais justa e equitativa. A estrutura jurídica da IA é fundamental para compreender como as leis e regulamentos podem ser utilizados para mitigar os impactos negativos da tecnologia, evitando lacunas

²⁴ FIDELIS, Vanderson Cadete; SOARES, DOUGLAS Verbicaro. **Os Desafios do Ordenamento Jurídico Brasileiro Frente às Deepfakes**. Revista Pensamento Jurídico, São Paulo, Brasil, v. 17, n. 1, 2023. Disponível em: <https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711>. Acesso em 09/05/2025.

²⁵ BRASIL. Senado Federal. **Projeto de Lei nº 2338, de 2023**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/162202>. Acesso em: 08/05/2025.

²⁶ FERREIRA, Laryssa Lopes. **Decolonizando O Futuro: Inteligência Artificial e Justiça Digital**. In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife(PE) Universidade Católica de Pernambuco, 2025. Disponível em: <https://www.even3.com.br/anais/publius/996149-DECOLONIZANDO-O-FUTURO--INTELIGENCIA-ARTIFICIAL-E-JUSTICA-DIGITAL>. Acesso em 08/05/2025

que podem ser exploradas para perpetuar desigualdades. Portanto, a legislação deve ser adaptada para lidar com as especificidades da IA garantindo que os desenvolvedores e usuários de IA sejam responsabilizados por suas ações, assegurando a conformidade e a proteção dos direitos dos indivíduos.

Temos ainda, dois Projetos de Lei do Senador Chico Rodrigues, onde o PL 145/2024²⁷ propõe a regulação no uso de IA para fins publicitários e a coibição de publicidade enganosa o que acarretaria crimes de falsa identidade e contra a honra, exigindo que o uso dessas ferramentas seja informado o que deve ser voltado para alteração dentro do Código de Defesa do Consumidor.

Já o PL 146/2024²⁸ que trata sobre da proposta de alteração ao Código Penal²⁹ (Decreto-lei 2.848, de 1940) tem o objetivo de aumentar as penas para crimes contra a honra cometidos em redes sociais utilizando *deepfakes* gerados por inteligência artificial. Aqueles que fizerem uso dessa tecnologia para criar vídeos ou imagens falsificadas poderão ter a pena, referente a crimes como calúnia ou difamação, multiplicada por cinco. As propostas, que foram apresentadas em fevereiro, já passaram pela designação das comissões e atualmente aguardam a designação dos relatores para análise e prosseguimento.

De acordo com o Senador Chico Rodrigues³⁰, "na seara do direito privado crescem as denúncias de personalidades que têm seu nome, voz e imagem vinculados a produtos e serviços, muitos dos quais de qualidade e segurança duvidosas".

Nesse contexto, a Constituição Federal³¹ reconhece os direitos à personalidade como fundamentais para a dignidade e integridade da seguinte forma:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Em complemento, vale destacar que também é essencial a responsabilização dos responsáveis pelas plataformas, criadores e disseminadores, definindo penas e multas específicas para aqueles que possibilitam, criam ou divulgam *deepfakes* com a intenção de causar danos ou enganar.

Neste cenário, o Supremo Tribunal Federal (STF), atualmente julga o Recurso Extraordinário 1037396³² o qual tem o reconhecido a Repercussão Geral, tema de relevância para todo o país, onde analisam o art. 19 da Lei 12.965/2014 (Marco Civil da Internet)³³ que trata dos provedores de internet, mas estendem, neste julgamento, o entendimento para websites, e gestores de redes sociais, por entenderem possível violação da Constituição Federal. O Tribunal Pleno do STF se reuniu pela última vez em 25 de junho de 2025 e, atualmente, o processo que trata da análise da responsabilidade da remoção de conteúdos falsos e ofensivos, encontra-se suspenso. O que evidencia a relevância do tema diante das novas particularidades no mundo digital promovido pela internet.

²⁷ BRASIL. Senado Federal. **Projeto de Lei nº 145/2024**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161946>. Acesso em 05/05/2025.

²⁸ BRASIL. Senado Federal. **Projeto de Lei nº 146/2024**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161947>. Acesso em 05/05/2025.

²⁹ BRASIL. **Código Penal**. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

³⁰ BRASIL. Senado Federal. **Projetos buscam restringir manipulação de imagens com inteligência artificial**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/02/07/projetos-buscam-restringir-manipulacao-de-imagens-com-inteligencia-artificial>. Acesso em 22/05/2025.

³¹ BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 05/05/2025.

³² BRASIL. **Supremo Tribunal Federal. Recurso Extraordinário n. 1.037.396 (Incidente n. 5160549 – Tema 987)**. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em 25/06/2025.

³³ BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 25/06/2025.

5.2 Atualização e Reforço das Normas Existentes

É necessário, além da legislação específica, adaptar e reforçar as leis existentes. Em primeiro lugar, a revisão do Código Penal deve incluir disposições que abordem explicitamente os crimes cometidos contra a produção e divulgação dos *deepfakes*, como falsidade ideológica e crimes contra a honra. Essa atualização é essencial para assegurar que a legislação penal cubra as novas formas de fraude e manipulação digital.

Também é importante ampliar a Lei Geral de Proteção de Dados³⁴, incorporando regulamentações que tratem diretamente da manipulação digital de dados pessoais, incluindo imagens e vozes. Essa ampliação deve ter como objetivo resguardar mais eficazmente as vítimas, garantindo uma cobertura mais completa para a privacidade e a integridade de informações pessoais.

A Lei de Delitos Informáticos³⁵ também necessita de ajustes. É crucial adaptar a lei para incluir a criação e disseminação de *deepfakes* como tipos específicos de crimes digitais. Essa adaptação permitirá uma resposta jurídica mais eficiente contra as ameaças emergentes associadas a essas tecnologias.

Nesse sentido, é fundamental reforçar que o uso das redes sociais para disseminar conteúdos manipulados, ainda que sob o argumento da liberdade de expressão assegurada no artigo 5º, inciso IV, da Constituição Federal³⁶ que garante ser “livre a manifestação do pensamento, sendo vedado o anonimato”, deve observar os limites legais e éticos. Como destacam Conceição *et al*³⁷:

Todo indivíduo é responsável por tudo que compartilha ou publica nas redes sociais, todavia devem estar cientes das consequências acarretadas pelos seus atos. Desse modo, é necessário sempre pensar que a liberdade de expressão, ainda que tenha finalidade de democracia e justiça social, deve ter como base o respeito à honra, à imagem, à privacidade e à ética na veracidade das informações. Vale ressaltar que a liberdade de expressão é um direito fundamental, tendo em vista que todo cidadão tem o direito de exercer essa garantia que a democracia proporciona no seu compartilhamento de conteúdo e publicações. Diante da manifestação de pensamento que a Constituição Federal oferece, não pode o indivíduo, pelo mau uso desse exercício, lesionar a honra e a imagem de outras pessoas, acarretando a sua responsabilização na esfera civil e criminal a respeito dos conteúdos ilícitos propagados na internet.

Essa compreensão se torna ainda mais relevante diante da constatação de que a proliferação de desinformação fragiliza os valores democráticos ao manipular a opinião pública, comprometendo a credibilidade das instituições e a formação de consensos sociais baseados em fatos. Assim, o desafio para as democracias contemporâneas reside justamente em regular as plataformas digitais e alcançar um equilíbrio entre liberdade de expressão e responsabilidade no compartilhamento de informações³⁸. A responsabilização do indivíduo, conforme destacado por Conceição *et al.*, precisa caminhar junto com a regulamentação efetiva dos espaços digitais, a fim de evitar que esses ambientes se tornem terrenos férteis para a desinformação e para práticas lesivas à dignidade humana.

A legislação, portanto, deve prever mecanismos claros para a reparação financeira, incluindo

³⁴ BRASIL. Lei Nº 13.709, de 14 de Agosto de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 07/05/2025.

³⁵ BRASIL. Lei Nº 12.737, de 30 de Novembro de 2012. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em 07/05/2025.

³⁶ BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 05/05/2025.

³⁷ CONCEIÇÃO, João Roberto da; SILVA, Patrícia Alves da; SANTOS, Alex de Freitas Barbosa dos; SENNA, Elisandra Vanessa do Nascimento; SILVA, Myllena Rebeka Avelino da. **Liberdade de expressão e a proteção constitucional da honra e imagem no âmbito das redes sociais**. *Revista Universitas Brasil*, v. 2, n. 2, p. 1–15, 24 abr. 2025. Disponível em: <https://revistaub.com/index.php/RUB/article/view/141/121>. Acesso em 06/05/2025.

³⁸ SENNA, Maria Luisa Souza Oliveira de; BARROSO, Fábio Túlio. **As Plataformas Digitais como Instrumento de Controle de Massas e Disseminação de Fake News: O Impacto da Cibercultura no Poder Político e nos Regimes Democráticos**. In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife(PE) Universidade Católica de Pernambuco, 2025. Disponível em: <https://www.even3.com.br/anais/publius/991591-AS-PLATAFORMAS-DIGITAIS-COMO-INSTRUMENTO-DE-CONTROLE-DE-MASSAS-E-DISSEMINACAO-DE-FAKE-NEWS--O-IMPACTO-DA-CIBERCUL>. Acesso em 08/05/2025.

indenizações por danos à reputação, privacidade e bem-estar psicológico. Além disso, a responsabilidade das plataformas digitais deve ser definida, incluindo a obrigação de implementar medidas eficazes de moderação e a colaboração com autoridades para identificar e sancionar os responsáveis. As empresas que desenvolvem ou distribuem ferramentas para criar conteúdos digitais falsos também devem ser responsabilizadas por seu uso inadequado, com a implementação de controles e práticas para prevenir abusos e a possibilidade de ações judiciais em casos de negligência e imperícia, devido à ausência de cuidado na supervisão ou controle de *deepfakes*.

5.3 Implementação de Tecnologias de Detecção

O avanço das ferramentas de detecção é essencial para combater os *deepfakes*, devendo ser uma prioridade. Primeiramente, é fundamental promover e financiar pesquisas em tecnologias de detecção, incentivando parcerias entre o setor público e privado. Esse apoio à pesquisa pode acelerar o desenvolvimento de medidas efetivas para identificar e mitigar os impactos desses conteúdos manipulados.

Tecnologias que possam ser utilizadas por plataformas de mídia social e instituições para identificar e verificar a autenticidade de conteúdos digitais são importantes para garantir a integridade das informações que circulam na internet. A implementação dessas ferramentas ajudará a prevenir a disseminação de informações falsas por meio de mecanismos audiovisuais e proteger o público de notícias falsas.

A educação também desempenha um papel vital no combate, pois a capacitação principalmente de profissionais de mídia, jornalistas e autoridades policiais no uso dessas ferramentas e na identificação de *deepfakes* é essencial para criar uma rede colaborativa de proteção mais robusta. Essa formação deve incluir não apenas o treinamento técnico, mas também a conscientização sobre as implicações legais e éticas associadas à manipulação digital.

5.4 Tribunal Superior Eleitoral: Iniciativa Pioneira na Regulação de Deepfakes

O Tribunal Superior Eleitoral (TSE) se destaca como uma das primeiras instituições no Brasil a adotar uma abordagem proativa na regulação do uso de *deepfakes* e outras tecnologias de manipulação digital no âmbito eleitoral, algo muito parecido com o que aconteceu no Texas e Califórnia (EUA) no ano de 2019. O TSE em 2024 estabeleceu exigências de que qualquer produção audiovisual que utilize IA para criar ou manipular imagens e vozes inclua uma sinalização clara para informar sobre o uso dessas tecnologias.

A adoção dessa medida ocorre diante de um cenário marcado pela circulação de desinformação e *deepfakes* nas redes sociais, fenômeno que desorienta a população, fragiliza a confiança nas instituições democráticas e põe em risco a legitimidade do processo eleitoral, conforme destacam Araújo, Moraes e Dias³⁹. Entre as medidas da norma, destaca-se a regulação do uso de *deepfakes*, a obrigação dos candidatos em rotular claramente qualquer conteúdo gerado por IA e, ainda, a obrigação das plataformas digitais em remover imediatamente conteúdos falsos.

Essa iniciativa visa combater a disseminação de conteúdos falsos que, por meio de *deepfakes*, podem parecer extremamente realistas e induzir os eleitores a acreditarem em informações que não correspondem à realidade. A regulamentação busca prevenir que produções enganosas distorçam a percepção pública, levando os eleitores a considerar situações fictícias que podem influenciar seu voto de forma errada.

Assim, o TSE, para garantir a lisura do processo eleitoral e combater a disseminação de informações falsas ou manipuladas, incluiu, na Resolução nº 23.732/2024⁴⁰, regras específicas sobre a utilização de

³⁹ ARAÚJO, Maria Quitéria Tavares de; MORAES, Éverton Gonçalves; DIAS, Rodolpho Cavalcanti. **A Inteligência Artificial como Ameaça à Democracia na era da Desinformação**. In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife (PE) Universidade Católica de Pernambuco, 2025. Disponível em: <https://www.even3.com.br/anais/publius/935981-A-INTELIGENCIA-ARTIFICIAL-COMO-AMEACA-A-DEMOCRACIA-NA-ERA-DA-DESINFORMACAO>. Acesso em: 06/05/2025.

⁴⁰ BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Resolução nº 23.610/2019, que dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral**. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em 07/05/2025.

conteúdo digital na propaganda eleitoral. A exemplo do

Art. 9º-C É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral.

§ 1º É proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia (deep fake).

§ 2º O descumprimento do previsto no caput e no § 1º deste artigo configura abuso do poder político e uso indevido dos meios de comunicação social, acarretando a cassação do registro ou do mandato, e impõe apuração das responsabilidades nos termos do § 1º do art. 323 do Código Eleitoral, sem prejuízo de aplicação de outras medidas cabíveis quanto à irregularidade da propaganda e à ilicitude do conteúdo.

Essas disposições refletem a crescente preocupação com o impacto das tecnologias de manipulação digital, como os *deepfakes*, no processo eleitoral, reforçando a necessidade de regulamentação para preservação da integridade. A resolução também traz em seu art. 9º-D sobre diversos outros aspectos como a responsabilização dos provedores de aplicação em que são obrigados a seguir determinadas regras de acordo com o descrito como termos de política de uso, instrumentos de notificação, canais de denúncia, ações corretivas e preventivas, pois ao identificar fatos nitidamente falsos deverão tomar providências imediatas e eficazes para interromper qualquer tentativa de continuidade.

Nas últimas eleições municipais da cidade de São Paulo, o candidato à prefeitura, Pablo Marçal, replicou um vídeo em sua rede social que foi inicialmente postado pela senhora Maiara Machado da Silva, a qual foi alvo de determinações judiciais para a remoção de vídeos manipulados envolvendo figuras políticas. No vídeo, o ex-presidente Jair Bolsonaro aparecia pedindo votos para Marçal, enquanto em outro, o atual presidente Luiz Inácio Lula da Silva e Guilherme Boulos, também candidato à prefeitura de São Paulo, eram mostrados dançando uma paródia. Tais vídeos foram considerados violações das normas descritas na Resolução nº 23.732/2024⁴¹ do TSE, pois utilizavam manipulações feitas por inteligência artificial de forma maliciosa, o que poderia desorientar o eleitorado.

Na decisão referente ao vídeo envolvendo Bolsonaro, requerida pelo então prefeito, Ricardo Nunes, que disputava a reeleição, o juiz da 2ª Zona Eleitoral, Rodrigo Marzola Columbini, confirmou a liminar que determinava a remoção do conteúdo. Ele destacou que “não precisa qualquer esforço intelectual para perceber que o vídeo impugnado é objeto de inteligência artificial não rotulada, como também de flagrante manipulação digital de áudio e vídeo”.

O juiz eleitoral também aplicou uma multa de R\$5.000 pela postagem do vídeo, por “divulgação de desinformação e *deepfake*”. O perfil foi identificado, porém, a pessoa responsável pelo perfil nega ter feito a publicação. Neste processo⁴² (0600205-05.2024.6.26.0002) não houve recurso da sentença, que já transitou em julgado e está em fase de cumprimento, com o parcelamento do débito.

É papel do TSE, conforme a Resolução, não só exigir a remoção de conteúdos ilegais, mas também garantir que os provedores publiquem informações que corrijam os efeitos da desinformação. A normativa permite, ainda, a suspensão de perfis e outras penalidades que forem necessárias, dependendo da gravidade da violação.

Tais medidas, além de garantir a integridade das informações eleitorais, também desempenham um papel crucial na preservação da imagem dos candidatos. Ao assegurar que os eleitores sejam informados sobre o uso de tecnologias de manipulação digital, o TSE protege os candidatos de ataques injustos e manipulações que poderiam prejudicar sua reputação e enganar o eleitorado. Dessa forma, a iniciativa não apenas combate a desinformação, mas também resguarda a credibilidade e a imagem dos candidatos,

⁴¹ BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Resolução nº 23.610/2019, que dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral.** Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em 07/05/2025.

⁴² BRASIL. Tribunal Superior Eleitoral. **Consulta Unificada – Processo nº 0600205-05.2024.6.26.0002.** Disponível em: <https://consultaunificadapje.tse.jus.br/#/public/resultado/0600205-05.2024.6.26.0002>. Acesso em 03/05/2025.

promovendo um ambiente eleitoral mais transparente e justo.

5.5 A Lei nº 15.123/2025 e o Reconhecimento dos Deepfakes como Forma de Violência Psicológica contra a Mulher

A crescente utilização de tecnologias baseadas em inteligência artificial, tem exigido uma resposta jurídica proporcional à gravidade de seus impactos. Em abril de 2025, o sistema jurídico brasileiro deu um passo importante nesse sentido com a sanção da Lei nº 15.123/2025⁴³, que alterou o artigo 147-B do Código Penal⁴⁴ para estabelecer uma causa de aumento de pena nos casos de violência psicológica contra a mulher praticada com o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima.

A legislação considera a violência psicológica como qualquer conduta que cause dano emocional à mulher, prejudique seu pleno desenvolvimento ou que vise degradar ou controlar suas ações, crenças e decisões. O dispositivo foi reforçado com a seguinte redação em parágrafo único: “*A pena é aumentada de metade se o crime é cometido mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima*”⁴⁵.

Essa modificação legislativa representa um marco significativo na proteção das mulheres diante de novas formas de violência digital. Casos que envolvem a manipulação de vídeos, áudios ou imagens com o intuito de humilhar, constranger, ameaçar ou difamar a vítima agora contam com previsão expressa no Código Penal, o que fortalece o enfrentamento jurídico das *deepfakes* quando utilizadas como instrumento de agressão psicológica em desfavor da mulher. A autora da proposta, evidencia que tais tecnologias vêm sendo empregadas para criar conteúdos falsos de cunho sexual que violam a dignidade e a saúde mental de mulheres e meninas, com impactos devastadores para suas vidas pessoais e sociais.

A promulgação dessa lei, portanto, demonstra sensibilidade do legislador à urgência de regular novas práticas abusivas oriundas do uso da inteligência artificial, especialmente no que tange à proteção de grupos vulneráveis, mas, ainda que represente um avanço importante, é necessário reconhecer que o Brasil caminha em passos lentos na adaptação de sua legislação às complexas e velozes transformações tecnológicas.

A regulamentação das *deepfakes*, sobretudo em outras esferas como a política, o mercado de trabalho, a segurança da informação e demais circunstâncias penais, ainda é incipiente. No entanto, a Lei nº 15.123/2025⁴⁶ em conjunto com o TSE constituem um bom começo e sinaliza a abertura de caminhos para um arcabouço legal mais robusto e alinhado aos desafios da era digital.

6. Conclusão

O estudo realizado permitiu identificar os principais desafios que os *deepfakes* impõem ao cenário jurídico brasileiro, destacando a necessidade de adaptações e aprimoramento das normas vigentes. A evolução tecnológica, especialmente no campo da inteligência artificial, ultrapassou as fronteiras das legislações atuais, expondo lacunas que comprometem a proteção dos direitos fundamentais, como a privacidade, a honra e a imagem.

A pesquisa demonstrou que, embora existam dispositivos legais aplicáveis, como o Código Civil⁴⁷,

⁴³ BRASIL. Lei Nº 15.123, de 24 de Abril de 2025. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 03/05/2025.

⁴⁴ BRASIL. Código Penal. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

⁴⁵ BRASIL. Lei Nº 15.123, de 24 de Abril de 2025. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 22/05/2025.

⁴⁶ BRASIL. Lei Nº 15.123, de 24 de Abril de 2025. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 03/05/2025.

⁴⁷ BRASIL. Código Civil. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 27/04/2025.

Penal⁴⁸ e a LGPD⁴⁹, estes instrumentos são insuficientes para lidar com a complexidade das manipulações digitais geradas por *deepfakes*, devido às lacunas existentes em nosso ordenamento jurídico. Além disso, a comparação com a legislação europeia, especialmente o caso de Portugal, evidencia a necessidade do Brasil trilhar caminhos que já foram e estão sendo percorridos por outros países os quais já adotaram medidas específicas para regular o uso de tecnologias de manipulação audiovisual.

Nesse contexto, uma legislação específica combinada com o desenvolvimento de tecnologias de detecção e a cooperação entre instituições públicas e privadas, nacionais e internacionais, se mostra essencial para combater essa prática de forma eficaz. As propostas de Projetos de Lei no Brasil, ainda em tramitação, representam um avanço importante, mas é necessária uma ação mais célere para garantir a segurança jurídica e a proteção dos cidadãos.

Assim, entende-se que o direito brasileiro precisa evoluir rapidamente para acompanhar as transformações digitais, garantindo uma abordagem jurídica que proteja não apenas os indivíduos, mas também a integridade do sistema de justiça e da ordem social diante dos impactos dos *deepfakes*, promovendo um ambiente jurídico seguro e responsivo diante das inovações tecnológicas.

Cabe ainda destacar que este projeto poderá incentivar pesquisas futuras que analisem, por exemplo, a necessidade de aprimorar a compreensão sobre os desafios jurídicos impostos pelos *deepfakes* na era digital, especialmente no contexto brasileiro. A investigação poderá possibilitar a identificação de lacunas legislativas e estratégias mais eficazes para a proteção dos direitos fundamentais diante das manipulações digitais. Além disso, espera-se que os resultados deste estudo inspirem, no futuro, novas iniciativas acadêmicas e regulatórias que promovam maior esclarecimento sobre o tema e que contribuam para um ambiente jurídico mais seguro e adaptado às inovações tecnológicas.

7. Referências

1. BRASIL. **Código Civil**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 27/04/2025.
2. PINHEIRO, Patrícia Peck; **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.
3. PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse**. TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.
4. TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico**. 5. Ed. São Paulo: Sairava Educação, 2020.
5. CHEHUEN NETO, J. A., ASSAD, I. M., BIGNOTO, T. C., LIMA, W. G., & VIEIRA, C. M; **A pesquisa científica e suas classificações**. In J. A. Chehuen Neto (Org.), Metodologia, modelos e estatística aplicados à pesquisa científica na área da saúde (pp. 76–101). Juiz de Fora: Editora UFJF, 2022. Disponível em <https://www2.ufjf.br/editora/wp-content/uploads/sites/113/2022/09/Metodologia-Modelos-e-Estat%C3%ADstica-1.pdf>. Acessado em 07/05/2025.
6. PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse**. TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.
7. PRADO, Magaly Parreira do. **Deepfake de áudio: manipulação simula voz real para retratar**

⁴⁸ BRASIL. **Código Penal**. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

⁴⁹ BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 07/05/2025.

- alguém dizendo algo que não disse.** TecCogs – Revista Digital de Tecnologias Cognitivas, n. 17, 2021. Disponível em <https://revistas.pucsp.br/teccogs/article/view/55977>. Acesso em 30/04/2025.
8. ALVES, B. M.; ARAÚJO, A. K. V.; CAVALCANTE, J. F.; GALDINO JÚNIOR, F. E.; RODRIGUES, L. H. L.; OLIVEIRA, P. H. S. de. **Análise da responsabilização criminal dos criadores e propagadores de “deep fakes” no ordenamento jurídico brasileiro.** *Caderno Pedagógico*, v. 21, n. 6, p. e4348, 2024. DOI: <https://doi.org/10.54033/cadpedv21n6-075>. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348>. Acesso em 09/05/2025.
 9. BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 08/05/2025.
 10. TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico.** 5. Ed. São Paulo: Saraiva Educação, 2020.
 11. PINHEIRO, Patrícia Peck; **Direito Digital.** 7. ed. São Paulo: Saraiva Educação, 2021.
 12. TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico.** 5. Ed. São Paulo: Saraiva Educação, 2020.
 13. BRASIL. **Código Penal.** Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.
 14. BRASIL. **Lei Nº 12.737, de 30 de Novembro de 2012.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 07/05/2025.
 15. PINHEIRO, Patrícia Peck; **Direito Digital.** 7. ed. São Paulo: Saraiva Educação, 2021.
 16. BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 07/05/2025.
 17. TEIXEIRA, Tarcísio; **Direito Digital e Processo Eletrônico.** 5. Ed. São Paulo: Sairava Educação, 2020.
 18. HOFFMANN-RIEM, Wolfgang; **Teoria Geral do Direito Digital: desafios para o direito.** Rio de Janeiro: Forense, 2021.
 19. PORTUGAL. **Lei N.º 58/2019.** Disponível em https://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=leis&artigo_id=&nid=2961&nversao=&tabela=leis. Acesso em 06/05/2025.
 20. PORTUGAL. **Decreto-Lei n.º 48/1995.** Aprova o Código Penal. Disponível em: <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675>. Acesso em 06/05/2025.
 21. BRASIL. **Código Civil.** Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 27/04/2025.
 22. BRASIL. **Código Penal.** Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.
 23. BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018.** Disponível em

- https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 07/05/2025.
24. FIDELIS, Vanderson Cadete; SOARES, DOUGLAS Verbicaro. **Os Desafios do Ordenamento Jurídico Brasileiro Frente às Deepfakes**. Revista Pensamento Jurídico, São Paulo, Brasil, v. 17, n. 1, 2023. Disponível em: <https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711>. Acesso em 09/05/2025.
 25. BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em 08/05/2025.
 26. FERREIRA, Laryssa Lopes. **Decolonizando o Futuro: Inteligência Artificial e Justiça Digital**. In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife(PE) Universidade Católica de Pernambuco, 2025. Disponível em: <https://www.even3.com.br/anais/publius/996149-DESCOLONIZANDO-O-FUTURO--INTELIGENCIA-A-RTIFICIAL-E-JUSTICA-DIGITAL>. Acesso em 08/05/2025
 27. BRASIL. Senado Federal. **Projeto de Lei nº 145/2024**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161946>. Acesso em 05/05/2025.
 28. BRASIL. Senado Federal. **Projeto de Lei nº 146/2024**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/161947>. Acesso em 05/05/2025.
 29. BRASIL. **Código Penal**. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.
 30. BRASIL. Senado Federal. **Projetos buscam restringir manipulação de imagens com inteligência artificial**. Disponível em <https://www12.senado.leg.br/noticias/materias/2024/02/07/projetos-buscam-restringir-manipulacao-d-e-imagens-com-inteligencia-artificial>. Acesso em 22/05/2025.
 31. BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 05/05/2025.
 32. BRASIL. **Supremo Tribunal Federal. Recurso Extraordinário n. 1.037.396 (Incidente n. 5160549 – Tema 987)**. Relator: Min. Dias Toffoli. Brasília, DF, julgamento em 25/06/2025. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em 25/06/2025.
 33. BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 25/06/2025.
 34. BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 07/05/2025.
 35. BRASIL. **Lei Nº 12.737, de 30 de Novembro de 2012**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 07/05/2025.
 36. BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 05/05/2025.
 37. CONCEIÇÃO, João Roberto da; SILVA, Patrícia Alves da; SANTOS, Alex de Freitas Barbosa dos; SENA, Elisandra Vanessa do Nascimento; SILVA, Myllena Rebeka Avelino da. **Liberdade de**

- expressão e a proteção constitucional da honra e imagem no âmbito das redes sociais.** *Revista Universitas Brasil*, v. 2, n. 2, p. 1–15, 24 abr. 2025. Disponível em: <https://revistaub.com/index.php/RUB/article/view/141/121>. Acesso em 06/05/2025.
38. SENNA, Maria Luisa Souza Oliveira de; BARROSO, Fábio Túlio. **As Plataformas Digitais como Instrumento de Controle de Massas e Disseminação de Fake News: O Impacto da Ciber cultura no Poder Político e nos Regimes Democráticos.** In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife(PE) Universidade Católica de Pernambuco, 2025. Disponível em: <https://www.even3.com.br/anais/publius/991591-AS-PLATAFORMAS-DIGITAIS-COMO-INSTRUMENTO-DE-CONTROLE-DE-MASSAS-E-DISSEMINACAO-DE-FAKE-NEWS--O-IMPACTO-DA-CIBERCUL>. Acesso em 08/05/2025
 39. ARAÚJO, Maria Quitéria Tavares de; MORAES, Éverton Gonçalves; DIAS, Rodolpho Cavalcanti. **A Inteligência Artificial como Ameaça à Democracia na era da Desinformação.** In: Anais do Publius 2024 - Congresso de Direito Constitucional: “Direito, Constituição e De(s)colonialidade Digital”. Anais...Recife (PE) Universidade Católica de Pernambuco, 2025. Disponível em <https://www.even3.com.br/anais/publius/935981-A-INTELEGENCIA-ARTIFICIAL-COMO-AMEACA-A-DEMOCRACIA-NA-ERA-DA-DESINFORMACAO>. Acesso em 06/05/2025.
 40. BRASIL. Tribunal Superior Eleitoral.. **Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Resolução nº 23.610/2019, que dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral.** Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em 07/05/2025.
 41. BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Resolução nº 23.610/2019, que dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral.** Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em 07/05/2025.
 42. BRASIL. Tribunal Superior Eleitoral. **Consulta Unificada – Processo nº 0600205-05.2024.6.26.0002.** Disponível em: <https://consultaunificadapje.tse.jus.br/#/public/resultado/0600205-05.2024.6.26.0002>. Acesso em: 03/05/2025.
 43. BRASIL. **Lei Nº 15.123, de 24 de Abril de 2025.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 03/05/2025.
 44. BRASIL. **Código Penal.** Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.
 45. BRASIL. **Lei Nº 15.123, de 24 de Abril de 2025.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 03/05/2025.
 46. BRASIL. **Lei Nº 15.123, de 24 de Abril de 2025.** Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em 03/05/2025.
 47. BRASIL. **Código Civil.** Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 27/04/2025.
 48. BRASIL. **Código Penal.** Disponível em

https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 02/05/2025.

49. BRASIL. **Lei Nº 13.709, de 14 de Agosto de 2018**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 07/05/2025.