I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL III

PAULO CEZAR DIAS

VALTER MOURA DO CARMO

FERNANDO GALINDO AYUDA

I61
Inteligência Artificial: Desafios da Era Digital III [Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Fernando Galindo Ayuda, Paulo Cezar Dias, Valter Moura do Carmo. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-097-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Inteligência Artificial e Sustentabilidade na Era Transnacional

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Inteligência Artificial. 3. Desafios da Era Digital. I International Experience Perugia – Itália. (1: 2025 : Perugia, Itália).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL III

Apresentação

APRESENTAÇÃO

O I International Experience – Perúgia – Itália foi realizado nos dias 28, 29 e 30 de maio de 2025, com o tema "Inteligência Artificial e Sustentabilidade na Era Digital". O Grupo de Trabalho (GT) "Inteligência Artificial: Desafios da Era Digital III" ocorreu nos dias 29 e 30 de maio, nos períodos vespertinos, na Universidade de Perúgia.

O GT destacou-se não apenas pela qualidade dos trabalhos apresentados, mas também pelo nível acadêmico dos autores — doutores, mestres, professores pesquisadores e seus alunos pós-graduandos. O evento também proporcionou um importante espaço de interlocução internacional, contando com a participação de renomados juristas e professores de instituições estrangeiras, como os Professores Doutores Roberto Cippitani (Universidade de Perúgia) e Fernando Galindo (Universidade de Zaragoza – Espanha), que enriqueceram os debates e contribuíram para o sucesso da atividade.

Foram apresentados 15 (quinze) artigos, os quais foram objeto de intenso debate presidido pelos coordenadores e enriquecido pela participação ativa do público presente na Faculdade de Direito de Perúgia – ITÁLIA.

A apresentação dos trabalhos permitiu discussões atualizadas e profícuas sobre temas como inteligência artificial, uso de dados pessoais, dever de informação, riscos e interações tecnológicas. As abordagens trataram dos desafios enfrentados pelas diversas linhas de pesquisa jurídica no estudo do futuro da regulação no Brasil, dos abusos relacionados à inteligência artificial e das possíveis soluções para a proteção de dados em um mundo globalizado.

As temáticas incluíram: tecnologias relacionadas a fake news, deepfakes e bots; compliance; a consideração do elemento humano na aplicação da I.A. nas decisões judiciais; a inteligência artificial como ferramenta de proteção no sistema de justiça criminal; o consentimento informado e o uso de dados pessoais; regulamentação e governança da I.A.; precarização do governo digital e aplicação da inteligência artificial em distintos setores jurídicos.

A seguir, apresenta-se a relação dos trabalhos que compõem este Grupo de Trabalho, acompanhados de seus respectivos autores:

1. CAPACIDADE ARTIFICIAL DAS MÁQUINAS E A EXIGÊNCIA DE TRANSFORMAÇÕES NA MANEIRA DO SABER DE PROFISSIONAIS, de Fernanda Conceição Pohlmann.

2. AI, VOCÊ ESTÁ AÍ? O PANORAMA JURÍDICO RELATIVO À (AUTO) IDENTIFICAÇÃO DA INTELIGÊNCIA ARTIFICIAL, de Gabriel Siqueira Eliazar de Carvalho, André Fortes Chaves e Marcello Silva Nunes Leite.

3. DEMOCRACIA EM REDE: O PAPEL DA INTELIGÊNCIA ARTIFICIAL E DOS ALGORITMOS NA LIBERDADE DE EXPRESSÃO E NO PLURALISMO POLÍTICO, de Kennedy da Nobrega Martins, Alexandre Manuel Lopes Rodrigues e Jadgleison Rocha Alves.

4. INTELIGÊNCIA ARTIFICIAL E DIREITOS FUNDAMENTAIS: DESAFIOS E TENSÕES NA ERA DIGITAL, de Jesualdo Eduardo de Almeida Junior e Gustavo Roberto Dias Tonia.

5. INTELIGÊNCIA ARTIFICIAL E DEMOCRACIA: O PERIGO DA MANIPULAÇÃO DE INFORMAÇÕES, de Claudia Maria da Silva Bezerra e Luiz Eduardo Simões de Souza.

6. INFLUÊNCIAS DO REALISMO JURÍDICO E O USO DA INTELIGÊNCIA ARTIFICIAL NA ELABORAÇÃO DE DECISÕES JUDICIAIS NO BRASIL: VIESES COGNITIVOS E HEURÍSTICAS NO PROCESSO DECISÓRIO, de Kerry Barreto, Fausto Santos de Morais e Júlia Regina Bassani Caus.

7. CRITÉRIOS QUANTITATIVOS PARA A MENSURAÇÃO DE RESULTADOS NO JUÍZO 100% DIGITAL: RISCOS PARA A QUALIDADE DA PRESTAÇÃO JURISDICIONAL NO BRASIL, de Orides Mezzaroba, José Renato Gaziero Cella e Lia Loana Curial Oliva.

8. AS PROVAS DIGITAIS NO PROCESSO CIVIL E O (DES)CABIMENTO DA CADEIA DE CUSTÓDIA, de Jesualdo Eduardo de Almeida Junior e Gustavo Roberto Dias Tonia.

9. A REVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL NOS GABINETES JUDICIAIS: EFICIÊNCIA COM GARANTIAS CONSTITUCIONAIS, de Lisbino Geraldo Miranda do Carmo, Deise Neves Nazaré Rios Brito e Jimmy Souza do Carmo.

10. GENEALOGIA E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL PARA ELABORAÇÃO DE UM ONOMÁSTICO DOS IMIGRANTES ITALIANOS QUE DESENVOLVERAM O SUL DO ESTADO DE SANTA CATARINA DE 1877 A 1897, de Júlio Cesar Cancellier de Olivo.

11. A REDE-LAB COMO INOVAÇÃO NA POLÍTICA ANTILAVAGEM DE CAPITAIS NO BRASIL, de Lorrayne Souza Galli e Matheus Felipe de Castro.

12. ARMAS AUTÔNOMAS LETAIS: OS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL PARA OS DIREITOS HUMANOS E SUA CONSEQUENTE REGULAMENTAÇÃO, de Alexandre Gonçalves Ribeiro e Renata Mantovani de Lima.

13. A INTELIGÊNCIA ARTIFICIAL COMO FERRAMENTA ESSENCIAL NA ELUCIDAÇÃO DE CRIMES SEXUAIS PRATICADOS COM VIOLÊNCIA CONTRA A MULHER, de Eneida Orbage de Britto Taquary e Catharina Orbage de Britto Taquary Berino.

14. A INTELIGÊNCIA ARTIFICIAL NO DIREITO PENAL: AVANÇOS, DESAFIOS E IMPACTOS NA INVESTIGAÇÃO E NO SISTEMA JUDICIAL, de Eneida Orbage de Britto Taquary, Bianca Cristina Barbosa de Oliveira e Tiago de Lima Mascarenhas Santos.

15. ENTRE CÓDIGOS E DIREITOS: UMA ANÁLISE CONSTITUCIONAL DA PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA INTELIGÊNCIA ARTIFICIAL, de Lisbino Geraldo Miranda do Carmo, Deise Neves Nazaré Rios Brito e Paulo Henrique da Silva Costa.

Por fim, os organizadores e coordenadores do Grupo de Trabalho "Inteligência Artificial: Desafios da Era Digital III" parabenizam e agradecem aos autores pelos valiosos trabalhos apresentados, cuja leitura certamente contribuirá para o aprofundamento do debate acadêmico e científico na área.

Prof. Dr. Fernando Galindo - Universidad de Zaragoza - Espanha

Prof. Dr. Valter Moura do Carmo – PPGPJDH - ESMAT e UFT

Prof. Dr. Paulo Cezar Dias – Centro Universitário Eurípides de Marília - SP

DEEPFAKES E INTELIGÊNCIA ARTIFICIAL: O CRIME DE DIFAMAÇÃO NA ERA DIGITAL E A REGULAÇÃO COMPARADA ENTRE BRASIL E CHINA

DEEPFAKES AND ARTIFICIAL INTELLIGENCE: THE CRIME OF DEFAMATION IN THE DIGITAL ERA AND THE COMPARATIVE REGULATION BETWEEN BRAZIL AND CHINA

Claudia Maria Da Silva Bezerra [1]
Diogo Vieira Pereira [2]
Lucas Carvalho Gadelha [3]

Resumo

O avanço da Inteligência Artificial (IA) tem transformado significativamente a comunicação digital, proporcionando inovações tecnológicas, mas também ampliando riscos jurídicos e sociais, especialmente no que tange à manipulação da realidade por meio dos deepfakes. Esse fenômeno representa um novo patamar para os crimes contra a honra, particularmente a difamação, permitindo a disseminação de informações falsas de maneira extremamente convincente e de difícil detecção. Este estudo analisa a utilização dos deepfakes como instrumento para a prática do crime de difamação, destacando seus impactos na honra e na reputação das vítimas no ambiente digital e investigando a resposta regulatória dos ordenamentos jurídicos do Brasil e da China. A pesquisa adota uma abordagem qualitativa, com revisão bibliográfica, documental e análise comparada, buscando compreender como cada país tem enfrentado esse desafio legislativo. Os resultados indicam que a China implementou um rigoroso arcabouço normativo, exigindo a identificação de conteúdos sintéticos e impondo sanções severas para o uso indevido dessa tecnologia. No Brasil, por outro lado, ainda não há regulamentação específica sobre deepfakes, o que gera insegurança jurídica e dificuldades na aplicação das normas existentes. Apesar de o Brasil dispor de instrumentos normativos como o Código Penal, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), esses mecanismos são insuficientes para lidar com a complexidade dos deepfakes. Assim, sugere-se um marco regulatório mais específico para garantir maior proteção à honra e à reputação das vítimas, além da implementação de medidas preventivas e educativas para mitigar os impactos dessa tecnologia.

Palavras-chave: Crimes contra a honra, Crimes digitais, Manipulação de imagens, Privacidade e segurança, Deepfake

---

[1] Pós-doutoranda em Direito PPGDIR-UFMA. Doutora e Mestre em Administração - UNINOVE. Editora Associada RIAE. Líder Sustentabilidade SINGEP/UNINOVE/SP. Líder Gestão Socio-ambiental/ODS-EMPRAD/FEA-USP. Pesquisadora NEDC/UFMA. Professora IDEA-DIREITO – São Luís/MA. E-mail: profa. claudiamsbezerra@gmail.com

[2] Mestre em Educação Física UFMA. Mestrando em Direito – UFMA. Advogado e Professor de Direito do Trabalho e Penal na Faculdade IDEA São Luís. E-mail: diogov_p@hotmail.com

[3] Graduando em Direito na Universidade Federal do Maranhão-UFMA, Brasil. Lucasgadelha101@gmail.com

Abstract/Resumen/Résumé

The advancement of Artificial Intelligence (AI) has significantly transformed digital communication, providing technological innovations while also increasing legal and social risks, particularly regarding the manipulation of reality through deepfakes. This phenomenon represents a new level of complexity for crimes against honor, particularly defamation, enabling the dissemination of false information in an extremely convincing and difficult-to-detect manner. This study analyzes the use of deepfakes as an instrument for committing defamation crimes, highlighting their impact on the honor and reputation of victims in the digital environment and investigating the regulatory responses of the legal systems of Brazil and China. The research adopts a qualitative approach, based on bibliographic and documentary review, as well as comparative analysis, seeking to understand how each country has addressed this legislative challenge. The results indicate that China has implemented a strict regulatory framework, requiring the identification of synthetic content and imposing severe penalties for the misuse of the technology. In contrast, Brazil still lacks specific regulations on deepfakes, leading to legal uncertainty and difficulties in enforcing existing laws. Although Brazil has normative instruments such as the Penal Code, the Civil Rights Framework for the Internet, and the General Data Protection Law (LGPD), these mechanisms are insufficient to address the complexity of deepfakes. Therefore, a more specific regulatory framework is suggested to ensure greater protection of victims' honor and reputation, as well as the implementation of preventive and educational measures to mitigate the negative impacts of this technology.

Keywords/Palabras-claves/Mots-clés: Crimes against honor, Digital crimes, Image manipulation, Privacy and security, Deepfake

1. INTRODUÇÃO

A revolução promovida pela Inteligência Artificial (IA) tem redefinido os limites entre o real e o virtual, gerando oportunidades para a comunicação e inovação, mas também introduzindo desafios jurídicos e éticos sem precedentes. Entre os fenômenos mais preocupantes da era digital, os *deepfakes* se destacam como uma tecnologia baseada em IA que permite a manipulação realista de imagens, áudios e vídeos. Essa técnica utiliza redes neurais profundas e algoritmos de aprendizado de máquina para falsificar rostos e vozes com notável precisão, simulando ações de pessoas em situações que nunca ocorreram. A sofisticação dos *deepfakes* tem tornado cada vez mais difícil diferenciar o verdadeiro do falso, o que gera implicações graves para a privacidade, a reputação e a confiabilidade das informações disseminadas no ambiente digital.

A utilização de *deepfakes* na prática de crimes contra a honra, especialmente na difamação, representa um desafio crescente para os sistemas jurídicos em todo o mundo. No Brasil, a legislação ainda carece de mecanismos específicos para lidar com esse fenômeno, enquanto a China já implementou regulamentações que impõem restrições rigorosas ao uso de tecnologias de síntese profunda. A análise comparativa entre os modelos regulatórios desses países é essencial para compreender como os ordenamentos jurídicos podem se adaptar à nova realidade digital e mitigar os impactos negativos da IA na produção e disseminação de conteúdos falsificados.

Ou seja, a China foi escolhida para este estudo comparado por seu pioneirismo na orientação das deepfakes, adotando uma abordagem estatal rigorosa para mitigar os impactos dessa tecnologia. Enquanto muitos países ainda discutem normas sobre o tema, a China implementou, em 10 de janeiro de 2023, as *Deep Synthesis Provisions* (*Provisions on the Administration of Deep Synthesis of Internet-based Information Services*), elaboradas pela *Cyberspace Administration of China* (CAC) em parceria com o Ministério da Indústria e Tecnologia da Informação (MIIT) e o Ministério da Segurança Pública (MPS). A análise desse modelo regulatório permite identificar lições e desafios para o Brasil, contribuindo para o debate sobre a governança das propriedades profundas.

Diante desse cenário, a pesquisa busca responder à seguinte questão: como os ordenamentos jurídicos brasileiro e chinês enfrentam o uso de *deepfakes* na prática da difamação e quais são os desafios regulatórios envolvidos? O presente estudo tem como objetivo analisar o uso dos *deepfakes* como ferramenta para a prática do crime de difamação, investigando de que forma essa tecnologia tem sido instrumentalizada para criar e disseminar

conteúdos falsificados que comprometem a honra e a reputação das vítimas. Além disso, busca-se compreender a efetividade das medidas regulatórias adotadas por Brasil e China, identificando lacunas e desafios para aprimorar a governança digital e coibir a instrumentalização da IA para fins ilícitos.

Para alcançar esses objetivos, essa pesquisa adotou uma metodologia qualitativa e exploratória, fundamentada em revisão bibliográfica, análise documental e pesquisa comparada. Justifica-se a escolha dessa abordagem por possibilitar a construção de um quadro analítico que permite compreender a dinâmica da regulação jurídica dos *deepfakes* e seus impactos na proteção da honra, além de identificar diferenças normativas entre Brasil e China (Creswell; Poth, 2016; Mezzaroba; Monteiro, 2017). O delineamento da pesquisa é descritivo-analítico e comparado, pois busca identificar padrões regulatórios e compará-los criticamente, considerando as abordagens legislativas distintas desses países (Queiroz; Feferbaum, 2021).

Os procedimentos de coleta de dados incluem pesquisa bibliográfica e documental. A revisão bibliográfica foi realizada por meio da consulta às bases de dados acadêmicas como Google Acadêmico, Scopus, Scielo e Web of Science, visando identificar artigos científicos, relatórios de organismos internacionais e literatura especializada sobre o tema. A pesquisa documental abrangeu o exame de legislações, normativas e diretrizes regulatórias aplicáveis, permitindo uma análise comparativa entre os sistemas jurídicos estudados. O critério de seleção das fontes considerou a relevância, atualidade e impacto na comunidade acadêmica e jurídica (Gustin; Dias; Nicácio, 2020; Queiroz; Feferbaum, 2021).

A análise dos dados foi conduzida com base em um método interpretativo-dogmático e comparado. Esse método permite a interpretação crítica dos textos normativos e doutrinários, além da construção de uma abordagem comparativa que possibilita identificar tendências, desafios e lacunas regulatórias na aplicação do direito aos *deepfakes* (Gustin; Dias; Nicácio, 2020). A interpretação normativa foi complementada pela análise das estratégias regulatórias implementadas em Brasil e China, fornecendo uma visão aprofundada das respostas institucionais ao problema da difamação via IA (Mezzaroba; Monteiro, 2017).

A pesquisa está organizada em três capítulos. O primeiro capítulo aborda os fundamentos teóricos dos crimes contra a honra, analisando sua evolução histórica. O segundo capítulo examina em profundidade o conceito de *deepfake*, discutindo suas aplicações lícitas e ilícitas, além de sua relação com a IA no contexto do crime de difamação. Por fim, o terceiro capítulo realiza uma análise comparada entre Brasil e China, investigando as estratégias regulatórias adotadas para mitigar os riscos associados ao uso indevido dos *deepfakes*, bem

como as perspectivas para o aprimoramento da governança digital no Brasil, considerando experiências internacionais bem-sucedidas.

Com isso, espera-se contribuir para o debate sobre a necessidade de regulamentação da Inteligência Artificial no combate à desinformação e proteção dos direitos fundamentais, reforçando a urgência de mecanismos eficazes para enfrentar os desafios impostos pelos *deepfakes* na era digital.

2. FUNDAMENTOS TÉORICOS DOS CRIMES CONTRA A HONRA

A honra é um dos bens jurídicos fundamentais tutelados pelo ordenamento jurídico brasileiro. Trata-se de um atributo inerente à personalidade do indivíduo, representando sua dignidade, reputação e respeito social. Segundo Nogueira (1995), a honra reflete o reconhecimento da integridade moral de uma pessoa tanto em sua percepção individual quanto na avaliação da sociedade.

No Brasil, a Constituição Federal de 1988, em seu artigo 5.º, inciso X, assegura expressamente a inviolabilidade da honra e da imagem das pessoas, garantindo a proteção desse direito fundamental (Brasil, 1988). Essa tutela constitucional fundamenta a normatização infraconstitucional dos crimes contra a honra, reforçando a necessidade de repressão a condutas que possam comprometer a dignidade individual.

Nesse contexto, Luiz Araujo e Vidal Júnior (1999, p.97) destacam que "a imagem assume a característica do conjunto de atributos cultivados pelo indivíduo e reconhecidos pelo conjunto social". Tal conceito, denominado de "imagem-atributo", vincula-se diretamente à honra, evidenciando que a reputação de um indivíduo na sociedade é um elemento essencial para sua identidade pessoal e social.

No âmbito infraconstitucional, o Código Penal Brasileiro (Decreto-Lei nº 2.848/1940), prevê três modalidades de crimes contra a honra: calúnia (art. 138), difamação (art. 139) e injúria (art. 140). Esses dispositivos buscam proteger a dignidade do indivíduo contra ofensas que possam macular sua reputação e reconhecimento social.

A calúnia ocorre quando alguém atribui falsamente a outra pessoa a prática de um crime. Já a injúria refere-se à ofensa à dignidade ou decoro de um indivíduo, sem a necessidade de imputação de um fato específico. Por sua vez, a difamação, foco deste estudo, caracteriza-se pela atribuição de um fato ofensivo à reputação de alguém, independentemente de sua veracidade (Greco, 2006).

Segundo Bitencourt (2017), a honra é um bem jurídico protegido tanto na esfera individual quanto coletiva, pois sua violação compromete não apenas o indivíduo atingido, mas

a estabilidade das relações sociais. A proteção à honra objetiva, resguardada pelo crime de difamação, visa evitar danos à imagem pública de um indivíduo perante terceiros, reforçando o caráter público desse delito.

A difamação distingue-se dos demais crimes contra a honra por não exigir que o fato atribuído à vítima seja falso ou criminoso. Conforme disposto no artigo 139 do Código Penal, a configuração desse crime ocorre sempre que um indivíduo imputa a outro um fato ofensivo à sua reputação perante terceiros (Brasil, 1940).

Nucci (2017) destaca que a consumação da difamação ocorre quando a imputação do fato desonroso se torna pública, sendo irrelevante a veracidade da informação. O dolo, ou seja, a intenção de macular a reputação da vítima, é elemento essencial para a tipificação da conduta. Bitencourt (2017, p.314), reforça essa concepção ao afirmar que:

> A proteção da honra, como bem jurídico autônomo, não constitui interesse exclusivo do indivíduo, mas da própria coletividade, que tem interesse na preservação da honra, da incolumidade moral e da intimidade, além de outros bens jurídicos indispensáveis para a harmonia social (2017, p.314).

Esse entendimento evidencia que o crime de difamação transcende a esfera individual, impactando a coletividade ao comprometer a confiabilidade e a credibilidade social das vítimas.

Nucci (2017) enfatiza que:

> "Difamar significa desacreditar publicamente uma pessoa, maculando-lhe a reputação. Nesse caso, mais uma vez, o tipo penal foi propositadamente repetitivo. Difamar já significa imputar algo desairoso a outrem, embora a descrição abstrata feita pelo legislador tenha deixado claro que, no contexto do crime do art. 139, não se trata de qualquer fato inconveniente ou negativo, mas sim de fato ofensivo à sua reputação. Com isso, excluiu os fatos definidos como crime – que ficaram para o tipo penal da calúnia – bem como afastou qualquer vinculação à falsidade ou veracidade dos mesmos. Assim, difamar uma pessoa implica divulgar fatos infamantes à sua honra objetiva, sejam eles verdadeiros ou falsos" (Nucci, 2017, p. 688).

Bitencourt (2017) reforça essa concepção ao afirmar que a difamação consiste na imputação de um fato determinado e objetivo, cuja notoriedade deve atingir, necessariamente, um terceiro, além da vítima. Esse requisito decorre da própria natureza do bem jurídico tutelado, qual seja, a reputação social do indivíduo, que se define pela percepção que os demais membros da sociedade possuem acerca de sua conduta e caráter, rompendo bens jurídicos, como a sua imagem e a sua privacidade. Assim, para que o crime se concretize, não basta que a ofensa atinja apenas a vítima em sua esfera íntima; é imprescindível que a imputação seja conhecida por outrem, uma vez que a lesão jurídica incide sobre a imagem pública do indivíduo na comunidade em que está inserido.

Por outro lado, a concepção de dignidade e respeito na tradição jurídica chinesa está profundamente enraizada nos princípios do "Confucionismo", que moldaram não apenas a organização social da China, mas também seu sistema jurídico e filosófico ao longo dos séculos. Nesse sentido, no contexto confucionista, a sociedade ideal se estrutura sobre a busca pela harmonia e estabilidade, valores considerados indispensáveis para o progresso coletivo. Ao contrário da tradição jurídica ocidental, que enfatiza a autonomia do indivíduo e a salvaguarda dos direitos fundamentais, a doutrina confucionista propõe que o bem-estar da coletividade deve prevalecer sobre os interesses individuais (Riegel, 2006).

No Direito Penal da República Popular da China, o direito à dignidade e à reputação é considerado de maior relevância jurídica do que a liberdade de expressão. Essa primazia decorre do entendimento de que a sociedade deve funcionar como um organismo coeso, no qual cada indivíduo desempenha um papel específico para garantir a estabilidade social e evitar conflitos. A liberdade de expressão, nesse contexto, não é um direito absoluto, mas um elemento que deve ser compatibilizado com o interesse coletivo (Spahn, 2006). Assim, a legislação chinesa impõe restrições ao discurso público que possa desestabilizar a ordem social, ofender a dignidade de terceiros ou comprometer o respeito às autoridades (Hostettler, 2009).

Em contraste, no ordenamento jurídico chinês, a difamação assume contornos distintos, uma vez que a honra não é concebida exclusivamente como um direito individual, mas também como um valor associado à estabilidade social e à ordem pública. Conforme dispõe o artigo 246 do Código Penal da República Popular da China:

> **Artigo 246**. Aqueles que insultarem abertamente outras pessoas com o uso da força ou outros métodos, ou aqueles que fabricarem histórias para difamar outros, se o caso for grave, serão sentenciados a até três anos de prisão, detenção criminal, supervisão ou privação de seus direitos políticos. " (China, 1997)
> **(Grifos do autor)**

Diferentemente do modelo ocidental, no qual a verdade pode ser utilizada como meio de defesa para afastar a tipificação penal, o direito chinês não admite a veracidade do fato como excludente da ilicitude. Esse entendimento se fundamenta na concepção confucionista de honra, que enfatiza a preservação da harmonia social e o respeito às instituições, de modo que a simples exposição pública de uma informação potencialmente desonrosa – ainda que verdadeira – pode ser considerada lesiva à reputação do indivíduo e, por extensão, à ordem pública (Hostettler, 2009).

Essa diferença estrutural reflete as bases filosóficas e políticas de cada ordenamento jurídico. Enquanto o Direito Penal Brasileiro tutela a honra objetiva como um direito individual, restringindo a punição à violação da reputação perante terceiros, o Direito Penal Chinês adota

uma abordagem mais ampla, considerando a difamação como uma ameaça não apenas ao indivíduo, mas ao equilíbrio social e político do Estado. Esse aspecto evidencia uma das principais distinções entre os modelos jurídicos ocidental e oriental, influenciados, respectivamente, por princípios liberais de autonomia individual e por preceitos coletivistas baseados na harmonia e estabilidade da sociedade.

Nesta senda, é importante destacar que, com o avanço das tecnologias de comunicação, os crimes contra a honra passaram por uma significativa reconfiguração. A difamação digital apresenta peculiaridades que ampliam seus impactos e tornam sua repressão mais complexa. O meio virtual possibilita a rápida disseminação de informações ofensivas, dificultando a identificação dos responsáveis e a remoção dos conteúdos difamatórios (Silva, 2020).

Embora o Marco Civil da Internet (Lei nº 12.965/2014) estabeleça princípios e diretrizes para a proteção da honra e imagem no ambiente digital, atribuindo responsabilidades aos provedores de serviços online, bem como, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) contribua para a preservação da reputação digital dos indivíduos, impondo limites ao tratamento de informações pessoais que possam ser utilizadas de maneira difamatória (Brasil, 2014; 2018).

A regulação desses crimes ainda apresenta desafios, especialmente diante do crescimento de *deepfakes* e outras formas sofisticadas de manipulação digital. A ausência de legislação específica para lidar com a difamação decorrente de tecnologias avançadas, como a Inteligência Artificial, demonstra a necessidade de aprimoramento normativo para garantir uma proteção mais eficaz à honra no ambiente digital.

O estudo dos crimes contra a honra revela a importância da tutela da reputação e dignidade individual na estrutura social. A difamação, enquanto forma de ofensa à honra objetiva, adquire contornos ainda mais complexos no ambiente digital, exigindo do ordenamento jurídico uma adaptação contínua para garantir sua efetiva repressão. O próximo capítulo aprofundará a análise sobre os *deepfakes* e seu impacto na difamação digital, explorando os desafios regulatórios e as soluções legislativas para lidar com essa nova realidade.

3. *DEEPFAKES* E SUA RELAÇÃO COM A IA NO CONTETXO DA DIFAMAÇÃO

Os *deepfakes* são uma tecnologia baseada em Inteligência Artificial que permite a criação e manipulação de conteúdos audiovisuais de forma altamente realista. A técnica utiliza redes neurais profundas e algoritmos de aprendizado de máquina (*machine learning*) para

substituir rostos, alterar expressões e modificar falas em vídeos e áudios, criando uma ilusão convincente de realidade (Faustino, 2018).

O termo "*deepfake*" surge da junção de *deep learning* (aprendizado profundo) e *fake* (falso), caracterizando conteúdos gerados artificialmente para parecerem autênticos (Faustino, 2018). Essas manipulações podem ser utilizadas tanto para fins legítimos quanto para finalidades ilícitas, tornando-se um desafio jurídico significativo.

Os algoritmos utilizados nos *deepfakes* operam com redes generativas adversárias (GANs - Generative Adversarial Networks), nas quais um modelo cria conteúdos falsificados enquanto outro avalia sua autenticidade, aperfeiçoando continuamente a simulação. Esse aprimoramento constante tem tornado cada vez mais difícil distinguir conteúdos verdadeiros dos manipulados (Chesney; Citron, 2019).

Embora tenham surgido inicialmente para aplicações legítimas, como no setor do entretenimento e da educação, os *deepfakes* rapidamente passaram a ser utilizados de maneira ilícita. No cinema, por exemplo, essa tecnologia foi empregada para recriar atores falecidos, como ocorreu no filme *Rogue One: Uma História Star Wars* (2016), que trouxe digitalmente o ator Peter Cushing décadas após seu falecimento (Medon, 2021). Em relação a este uso, o autor destaca que:

> Valendo-se de técnicas computacionais, viabilizou-se a chamada "reconstrução digital" da imagem do já falecido ator, o que desperta questionamentos, como a necessidade de autorização dos herdeiros para a reconstrução de sua imagem. Note-se, contudo, a peculiaridade dessa situação: não se trata de reproduzir novamente imagens captadas em momento pretérito, mas de se criar novas imagens, a partir de capturas anteriores" (Medon, 2021, p.269)

Além disso, *deepfakes* podem ser utilizados para aprimorar a acessibilidade, auxiliando pessoas com deficiência auditiva na leitura labial e possibilitando a sintetização de voz com maior naturalidade. No campo educacional, a tecnologia permite recriar discursos históricos, proporcionando experiências imersivas para estudantes e pesquisadores (Chesney; Citron, 2018).

Apesar dessas aplicações positivas, o uso indevido dos *deepfakes* tem se tornado uma preocupação global. A disseminação de desinformação é uma das principais consequências, visto que vídeos manipulados podem ser utilizados para fabricar declarações falsas de figuras públicas, influenciar eleições e espalhar notícias enganosas.

Segundo Chesney e Citron (2018) a disseminação das *deepfakes* é impulsionada por três fatores principais: a velocidade de viralização nas redes sociais, a dificuldade de identificação dos conteúdos falsificados e a tendência humana à disseminação de informações impactantes. Pesquisas indicam que conteúdos falsos se espalham 70% mais rápido do que

notícias verdadeiras, devido ao seu alto apelo sensacionalista e à tendência humana de compartilhar informações impactantes (Correio Braziliense, 2018). Esse fenômeno, amplificado pelo funcionamento dos algoritmos das plataformas digitais, contribui para que *deepfakes* se tornem ferramentas eficazes de manipulação da opinião pública.

Assim como ocorreu com softwares de edição de imagem, como o *Photoshop*, ferramentas de criação de *deepfakes* estão se tornando acessíveis ao público geral, permitindo que qualquer pessoa, sem conhecimento técnico avançado, consiga produzir conteúdos falsificados de forma convincente. Essa democratização da tecnologia amplia o risco de seu uso indevido, visto que possibilita criminosos a criarem falsificações altamente sofisticadas para enganar vítimas, influenciar eleições e até mesmo manipular provas em processos judiciais. O impacto dessa manipulação se reflete diretamente no aumento de crimes contra a honra, especialmente a difamação, uma vez que a reputação de indivíduos pode ser comprometida de forma irreversível.

Dessa forma, a preocupação central em relação ao uso indevido do *deepfake* reside na sua instrumentalização em disseminar informações falsas que potencializa significativamente o alcance e o impacto dessas ofensas, pois os conteúdos manipulados adquirem um grau elevado de credibilidade, tornando-se difícil distinguir o real do falso. Portanto, o conteúdo falso gera uma ilusão de realidade, fazendo com que aqueles que o assistem não ajam por descompromisso com a verdade, mas sim porque realmente acreditam naquilo que está sendo exibido. Esse efeito ocorre devido ao alto grau de realismo e à capacidade de convencimento proporcionada pelas Deep fakes. Neste sentido, Chesney e Citron (2018) destacam que:

> A despersonificação digital é cada vez mais realista e convincente. A tecnologia falsa é a ponta dessa tendência. Ele utiliza algoritmos de aprendizado de máquina para inserir rostos e vozes em gravações de vídeo e áudio de pessoas reais e permite a criação de representações realistas a partir do tecido digital inteiro. O resultado final é um vídeo ou áudio realista que parece que alguém disse ou fez alguma coisa. Apesar de falsificações profundas poderem ser criadas com o consentimento das pessoas que aparecem, mais frequentemente elas serão criadas sem elas. Esta parte descreve a tecnologia e as forças garantindo sua difusão, viralidade e entrincheiramento (Chesney e Citron, 2018, p.06).

Além do impacto devastador na reputação e na honra, *Deepfakes* também têm sido utilizados para criar falsas declarações atribuídas a figuras públicas. Um exemplo disso foi um vídeo manipulado no qual Mark Zuckerberg, CEO do Facebook, aparece afirmando que tem controle sobre bilhões de dados roubados, segredos e futuros das pessoas, graças a uma exposição de arte chamada Spectre (Alecrim, 2019). Outro exemplo relevante é o caso das

eleições presidenciais na Argentina, em que a Uol[1] noticiou que grupos de direita e integrantes do partido de Javier Milei, La Libertad Avanza, compartilharam nas redes sociais um vídeo em que o adversário Sérgio Massa aparece supostamente consumindo cocaína, afetando sua imagem diante da população (Dauer,2024).

Outro impacto significativo está relacionado à pornografia não consensual. De acordo com um relatório da Sensity AI (2019), 96% dos vídeos *deepfake* disponíveis na internet são de conteúdo pornográfico, sendo as mulheres as principais vítimas desse tipo de abuso. Casos emblemáticos incluem a manipulação de imagens de jornalistas e ativistas, como aconteceu com a indiana Rana Ayyub, que teve sua reputação gravemente comprometida por um *deepfake* pornográfico disseminado em retaliação a suas críticas políticas (Ayyub, 2018).

O grande desafio dos *deepfakes* reside na dificuldade de identificação e rastreamento. Os métodos convencionais de verificação de fatos se mostram ineficazes diante do nível de sofisticação dessas falsificações, exigindo o desenvolvimento de softwares especializados para autenticação de conteúdo digital. Contudo, mesmo com ferramentas avançadas, a remoção de *deepfakes* da internet é um processo lento e burocrático, permitindo que seu impacto persista mesmo após sua detecção. Além disso, há uma lacuna legislativa significativa na maioria dos países, dificultando a responsabilização dos infratores (Ramos-Zaga, 2024).

Importante ressaltar, o papel fundamental das plataformas digitais na contenção dos impactos negativos dos *deepfakes*. Empresas como Facebook, Twitter e YouTube têm adotado políticas mais rígidas para moderar esse tipo de conteúdo, mas os desafios permanecem. Em 2020, o Facebook anunciou restrições à manipulação de vídeos, mas essas medidas não impediram que *deepfakes* fossem amplamente utilizados para desinformação durante processos eleitorais ao redor do mundo (Dauer, 2024). Contudo, a falta de regulamentação clara sobre a responsabilidade das plataformas em relação à moderação desses conteúdos continua sendo um tema controverso no debate jurídico global.

No Brasil, por exemplo, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) oferece certa proteção contra o uso indevido de imagens e dados pessoais, mas ainda não há uma tipificação penal específica para crimes envolvendo *deepfakes*. O Código Penal prevê sanções para difamação (art. 139), mas sua aplicação nesses casos depende de interpretações ampliadas, o que gera insegurança jurídica, contudo, importante salientar que o

[1] Disponível em: https://noticias.uol.com.br/confere/ultimas-noticias/2024/03/03/*deepfake*-uso-inteligencia-artificial-eleicoes-argentina-estados-unidos.htm. Acesso em 17/02/2025 às 15h.

art. 141, em seu §2º, do mesmo Diploma Legal, triplica a pena quando o crime for cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores.

Em contraste, a China tem sido pioneira na regulamentação dos *deepfakes*. O governo chinês impôs diretrizes rigorosas que exigem que plataformas digitais rotulem conteúdos sintéticos e restrinjam o uso da tecnologia para fins enganosos. As empresas de tecnologia são obrigadas a implementar mecanismos de detecção e sinalização de *deepfakes*, sob pena de sanções severas (Hemrajani, 2023). Essa abordagem evidencia um caminho possível para o Brasil, que ainda debate propostas legislativas para enfrentar esse fenômeno.

O avanço dos *deepfakes* representa um dos maiores desafios contemporâneos para a proteção da honra e da reputação no ambiente digital. Embora essa tecnologia tenha aplicações legítimas, seu uso ilícito tem se expandido de maneira alarmante, exigindo respostas legislativas rápidas e eficazes. A regulação dos *deepfakes* precisa equilibrar inovação tecnológica e segurança jurídica, garantindo que a Inteligência Artificial seja utilizada de forma ética e responsável. O próximo capítulo analisará a regulação comparada entre Brasil e China, destacando os desafios enfrentados e as estratégias adotadas para mitigar os impactos negativos dessa tecnologia.

4. REGULAÇÃO COMPARADA ENTRE BRASIL E CHINA: DESAFIOS E PERSPECTIVAS NO COMBATE ÀS *DEEPFAKES*

O avanço da inteligência artificial trouxe consigo desafios jurídicos significativos, sobretudo no que concerne à disseminação de desinformação e à manipulação da realidade por meio do *Deepfakes* (Robl Filho; Marrafon; Medón, 2022). De acordo com os autores, no cenário internacional, diferentes países têm adotado abordagens regulatórias para conter os riscos associados ao uso indevido dessa tecnologia. Enquanto o Brasil ainda debate propostas legislativas para tipificar e penalizar condutas relacionadas ao uso de inteligência artificial, a China já implementou um arcabouço normativo rigoroso, tornando-se pioneira na regulação dessa tecnologia (Jia, 2024).

A China foi um dos primeiros países a adotar uma regulamentação abrangente sobre *deepfakes*, com o objetivo de estabelecer diretrizes rigorosas para o uso e desenvolvimento da tecnologia de síntese profunda. Em vigor desde 10 de janeiro de 2023, a regulamentação, conhecida *Deep Synthesis Provisions (*Provisions on the Administration of Deep Synthesis of Internet-based Information Services) foi elaborada pela *Cyberspace Administration of China (CAC)* em conjunto com o Ministério da Indústria e Tecnologia da Informação (MIIT) e o

Ministério da Segurança Pública (MPS), estabelecendo parâmetros específicos para a aplicação de *deepfakes* na internet (China's Briefing News, 2022).

A regulamentação foi motivada por preocupações crescentes quanto ao impacto da inteligência artificial na integridade da informação e na confiança social, já que a democratização da tecnologia tem facilitado seu uso para fins ilícitos, como fraudes, manipulação política e ataques difamatórios. Um caso emblemático ocorreu em abril de 2022, quando um residente da cidade de Wenzhou, na China, denunciou ter sido vítima de um golpe no qual criminosos utilizaram tecnologia de substituição facial para se passarem por um amigo e solicitar dinheiro emprestado. Como resultado, a vítima sofreu um prejuízo superior a R$ 37,5 mil na transação fraudulenta (Possa, 2023).

As disposições exigem que qualquer alteração feita por IA em informações biométricas, como rostos e vozes, seja claramente identificada e acompanhada de consentimento do indivíduo afetado. Além disso, os provedores de serviços de síntese profunda devem implementar medidas de segurança, incluindo registro de usuários, auditoria de algoritmos, revisão ética e mecanismos de refutação de rumores, prevenindo assim a disseminação de desinformação (Finlayson-Brown; Ng, 2023).

Em paralelo a isso, destacam-se os principais artigos de forma traduzida do tal regulamento chinês:

> **Disposições sobre a Gestão da Síntese Profunda dos Serviços de Informação da Internet:**
> **Artigo 1** Estas Disposições são formuladas de acordo com a Lei de Segurança Cibernética da República Popular da China, a Lei de Segurança de Dados da República Popular da China, a Lei de Proteção de Informações Pessoais da República Popular da China, as Medidas de Gestão de Serviços de Informação da Internet e outras leis e regulamentos administrativos, a fim de fortalecer a gestão integrada aprofundada dos serviços de informação da Internet, promover os valores socialistas essenciais, salvaguardar a segurança nacional e os interesses públicos sociais e proteger os direitos e interesses legítimos dos cidadãos, pessoas jurídicas e outras organizações**.**
> **(...)**
> **Artigo 4** Ao fornecer serviços de síntese profunda, deve-se obedecer às leis e regulamentos, respeitar a moralidade social e os padrões éticos, aderir à direção política correta, à orientação da opinião pública e à orientação de valores, e promover o avanço e a qualidade dos serviços de síntese profunda.
> **(...)**
> **Artigo 6** Nenhuma organização ou indivíduo pode usar o Serviço de Síntese Profunda para produzir, copiar, publicar ou disseminar informações proibidas por leis e regulamentos administrativos, ou usar o Serviço de Síntese Profunda para se envolver em atividades proibidas por leis e regulamentos administrativos, como colocar em risco a segurança e os interesses nacionais, prejudicar a imagem nacional, infringir os interesses públicos sociais, perturbar a ordem econômica e social ou infringir os direitos e interesses legítimos de terceiros.
> Provedores e usuários de serviços de síntese profunda não devem usar serviços de síntese profunda para produzir, copiar, publicar ou disseminar informações falsas. Ao reimprimir informações de notícias produzidas e divulgadas com base em serviços de

> síntese profunda, as informações de notícias divulgadas pela unidade de fonte de informações de notícias da Internet devem ser reimpressas de acordo com a lei.
> **Artigo 7** Os provedores de serviços de síntese profunda devem implementar a responsabilidade principal pela segurança da informação, estabelecer e melhorar sistemas de gestão como registro de usuários, revisão de mecanismos de algoritmos, revisão de ética científica e tecnológica, revisão de divulgação de informações, segurança de dados, proteção de informações pessoais, fraude de rede anti-telecomunicações e resposta a emergências, e ter medidas de garantia técnica seguras e controláveis.
> **(...)**
> **Artigo 11** Os provedores de serviços de síntese profunda devem estabelecer e melhorar um mecanismo de refutação de rumores. Se descobrirem que informações falsas estão sendo produzidas, copiadas, publicadas ou disseminadas usando serviços de síntese profunda, devem tomar medidas oportunas de refutação de rumores, preservar registros relevantes e reportar ao departamento de segurança cibernética e informatização e às autoridades competentes relevantes.
> **Artigo 13** As lojas de aplicativos da Internet e outras plataformas de distribuição de aplicativos devem implementar responsabilidades de gerenciamento de segurança, como revisão de listagem, gerenciamento diário e resposta a emergências, e verificar a avaliação de segurança e o arquivamento de aplicativos de síntese profunda; para aqueles que violam os regulamentos nacionais relevantes, medidas oportunas, como não listagem, avisos, suspensão de serviços ou remoção, devem ser tomadas. (*Cyberspace Administration of China*, 2022) **(Grifo do autor)**

No Brasil, por outro lado, ainda não existe uma legislação específica para regular o uso de *deepfakes*. O ordenamento jurídico brasileiro contém princípios e normativas que protegem a privacidade e a inviolabilidade da intimidade, mas não há uma tipificação penal clara para crimes envolvendo *deepfakes*. O Código Penal Brasileiro, promulgado em 1940, não previa os desafios decorrentes da revolução digital. A Constituição Federal de 1988 protege a honra e a imagem das pessoas, mas a regulamentação do ambiente digital só começou a ser estruturada com o Marco Civil da Internet (Lei n.º 12.965/2014), que estabelece diretrizes sobre direitos e deveres no uso da internet, incluindo a proteção à privacidade e à intimidade, conforme disposto nos artigos 3º e 7º:

> **Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:**
> II - Proteção da privacidade
> (...)
> **Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:**
> I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 2014) **(Grifos do autor)**.

Desse modo, a elaboração desta legislação buscou estabelecer preceitos quanto à "necessidade de proteção específica de direitos, passando por temáticas como apuração de responsabilidade civil e criminal dos provedores, proteção dos usuários como consumidores e manutenção da rede" (Sangoi, 2016, p. 22).

Em outro contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. º 13.709/2018, trouxe avanços significativos ao estabelecer regras mais rígidas para o tratamento

de dados pessoais, garantindo maior segurança digital. Embora não tenha revogado expressamente dispositivos do Marco Civil da Internet (Lei n. º 12.965/2014), a LGPD promoveu uma alteração substancial na regulamentação da privacidade digital, consolidando a proteção de informações pessoais como um direito fundamental (Brasil, 2018).

No entanto, apesar de proteger a privacidade dos indivíduos, a LGPD não trata diretamente do uso indevido de *deepfakes* para a prática de crimes contra a honra e manipulação da informação. Os tribunais brasileiros têm utilizado legislações já existentes para enquadrar casos envolvendo *deepfakes*. Juristas têm interpretado dispositivos do Código Penal e do Marco Civil da Internet para punir autores de crimes cometidos por meio dessa tecnologia, mas a falta de um marco normativo específico gera insegurança jurídica.

Molina e Berenguel (2022) apontam que a legislação brasileira não prevê expressamente a criminalização dos *deepfakes*, levando os tribunais a recorrerem a diferentes normas para lidar com casos concretos, tais como a Lei Federal n.º 12.735/2012 (Lei Azeredo), Lei Federal n.º 12.737/2012 popularmente conhecida como Lei Carolina Dickmann, Lei Federal n.º 12.965/2014 (Marco Civil da Internet); Lei Federal n.º 13.718/2018 oriunda do Projeto de Lei n.º 5.555/2013, Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, Lei Federal n.º 13.853/2019. Além dos tipos penais descritos na Lei de Crimes Financeiro (Lei Federal n.º 7.492/86), Lei de Falências (Lei Federal n.º 11.101/2005), Código Eleitoral (Lei Federal n.º 4737/65) e principalmente nos crimes contra a honra (artigos 138/145 do Código Penal) e dignidade sexual (artigos 213/235 ‘c’ do Código Penal).

Atualmente, O Congresso Nacional tem pelo menos 46 projetos de lei em tramitação que visam regulamentar o uso da inteligência artificial (IA) no Brasil, refletindo a crescente preocupação com os impactos dessa tecnologia na sociedade. A agenda de regulamentação, considerada prioritária pelo presidente do Congresso, senador Rodrigo Pacheco (PSD-MG), busca estabelecer diretrizes para o uso responsável da IA prevenindo abusos e protegendo direitos fundamentais (Amorozo,2024).

Diante da necessidade premente de conscientizar a população sobre os riscos dessa tecnologia e instruindo sobre como identificar e combater conteúdos manipulados digitalmente, o Supremo Tribunal Federal (STF) lançou, em outubro de 2024, o *Guia Ilustrado Contra as Deepfakes*, uma iniciativa do Programa de Combate à Desinformação em parceria com a organização *Data Privacy* Brasil (Brasil, 2024).

O presidente da Corte, ministro Luís Roberto Barroso, enfatizou que as *deepfakes* representam um problema crescente, tornando a distinção entre real e fabricado cada vez mais

desafiadora[2]. Além disso, destacou a necessidade de educação midiática para combater a difusão de desinformação e discurso de ódio. O guia didático reforça a importância da verificação crítica de informações antes de compartilhá-las, alertando para os desafios que a tecnologia impõe à democracia e aos direitos fundamentais.

Neste sentido, um dos principais desafios no Brasil é o impacto dos *deepfakes* em campanhas eleitorais. O Tribunal Superior Eleitoral (TSE), diante do potencial dessa tecnologia para disseminação de desinformação, aprovou em fevereiro de 2024 alterações na Resolução nº 23.610/2019, estabelecendo novas regras para a propaganda eleitoral, proibindo o uso de *deepfakes* em campanhas e exigindo a inclusão de avisos explícitos quando houver uso de IA em materiais eleitorais (BRASIL, 2024).

Assim, a comparação entre os modelos regulatórios de Brasil e China evidencia a necessidade de uma legislação mais robusta para enfrentar os desafios trazidos pelos *deepfakes*. Enquanto o governo chinês adotou medidas preventivas, impondo restrições rigorosas ao uso dessa tecnologia, o Brasil ainda enfrenta dificuldades para estabelecer normas específicas. A experiência chinesa demonstra que a regulamentação eficiente deve incluir mecanismos de autenticação obrigatória, responsabilização das plataformas digitais e sanções rigorosas para a disseminação de conteúdos manipulados.

Diante desse panorama, o Brasil pode se beneficiar da experiência chinesa para aprimorar sua legislação. A implementação de diretrizes que exijam a identificação de conteúdo gerados por IA, aliada a um fortalecimento das penalidades para o uso ilícito dessa tecnologia, pode contribuir para a proteção da honra e da reputação no ambiente digital. Além disso, a criação de parcerias entre o setor público e empresas de tecnologia para o desenvolvimento de ferramentas de detecção e rastreamento de *deepfakes* pode ser uma alternativa viável para conter a disseminação de desinformação.

Portanto, o avanço da regulamentação dos *deepfakes* no Brasil é essencial para garantir um ambiente digital mais seguro e confiável. A adaptação do ordenamento jurídico às novas realidades tecnológicas permitirá não apenas a punição de infratores, mas também a prevenção do uso indevido da inteligência artificial, protegendo a integridade da informação e a segurança dos cidadãos.

Assim sendo, a abordagem chinesa, ao estabelecer uma legislação robusta para o controle dessa tecnologia, demonstra um esforço estatal para prevenir o uso indevido da

[2] Disponível em: https://noticias.stf.jus.br/postsnoticias/supremo-lanca-guia-ilustrado-contra-as-deepfakes/. Acesso em 17/02/2025 às 23h.

inteligência artificial, impondo mecanismos de verificação para evitar manipulações digitais prejudiciais. Por outro lado, o Brasil ainda carece de uma legislação específica para a criminalização das *Deepfakes*, recorrendo a normativas já existentes. Assim, é imperativo que o Direito acompanhe esse avanço tecnológico, estabelecendo regulações específicas para coibir seu uso indevido e garantir a segurança jurídica e informacional da sociedade.

5. CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar o uso da tecnologia *deepfake* como instrumento para a prática do crime de difamação, previsto no artigo 139 do Código Penal, bem como seus impactos na honra e reputação das vítimas. Para tanto, foi realizada uma análise comparativa entre as abordagens regulatórias adotadas pelo Brasil e pela China, identificando os desafios enfrentados por ambos os países na contenção desse fenômeno tecnológico Os resultados apontaram que, enquanto a China implementou uma legislação específica com restrições e mecanismos de controle rigorosos, o Brasil ainda não dispõe de um marco normativo direcionado ao combate dessa prática, recorrendo a dispositivos legais já existentes para sua tipificação e repressão.

A questão central que norteou a pesquisa foi compreender como o ordenamento jurídico brasileiro trata o uso de *deepfakes* no contexto da difamação e quais medidas podem ser adotadas para aprimorar sua regulação. A pesquisa revelou que, embora não haja uma legislação específica, o país dispõe de normas que podem ser aplicadas para responsabilizar aqueles que produzem e disseminam conteúdos falsificados, como o Código Penal, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, tais dispositivos se mostram insuficientes diante da constante evolução tecnológica e da velocidade com que os *deepfakes* se propagam, evidenciando a necessidade de um arcabouço normativo mais robusto para garantir uma resposta jurídica eficaz.

Dentre as contribuições teóricas deste estudo, destaca-se o aprofundamento do debate sobre os desafios impostos pela inteligência artificial ao direito penal e à proteção da honra. A pesquisa possibilitou uma visão crítica da regulamentação comparada, permitindo compreender diferentes abordagens normativas e suas implicações. Como principal contribuição prática, a discussão aqui apresentada reforça a importância da conscientização sobre os riscos jurídicos e sociais relacionados aos *deepfakes*, ressaltando a urgência de um marco regulatório específico que assegure maior segurança jurídica às vítimas e previna danos à reputação e à privacidade.

Apesar das contribuições, algumas limitações devem ser reconhecidas. O estudo concentrou-se na análise normativa e comparativa entre Brasil e China, sem abordar em

profundidade a experiência de outros países que também avançam nesse campo. Além disso, a rápida evolução da tecnologia pode tornar algumas das discussões aqui apresentadas defasadas em curto prazo, exigindo um monitoramento contínuo das iniciativas regulatórias e das novas diretrizes internacionais sobre inteligência artificial e manipulação digital.

Para estudos futuros, sugere-se uma investigação mais aprofundada sobre os impactos dos *deepfakes* no cenário eleitoral, considerando que essa tecnologia tem sido utilizada para influenciar a opinião pública e comprometer a integridade de campanhas políticas. Além disso, é recomendável explorar a viabilidade de ferramentas tecnológicas que possam ser incorporadas ao ordenamento jurídico para a detecção e remoção automatizada de conteúdos manipulados. Além disso, novas pesquisas podem examinar as implicações dos *deepfakes* no âmbito do direito civil, especialmente no que diz respeito à reparação de danos à imagem e à honra das vítimas. A experiência chinesa demonstra que a adoção de uma legislação específica pode ser uma estratégia eficaz para mitigar os efeitos dessa tecnologia, estabelecendo sanções claras e mecanismos de controle rigorosos. O Brasil pode se beneficiar dessas diretrizes ao estruturar um marco regulatório mais abrangente, que contemple não apenas penalidades para os responsáveis pela criação e disseminação de *deepfakes*, mas também medidas de prevenção e proteção às vítimas.

Dessa forma, espera-se que este estudo contribua para o avanço das discussões jurídicas sobre o tema, incentivando a adoção de medidas legislativas e regulatórias que promovam a segurança digital e garantam a proteção dos direitos fundamentais na era da inteligência artificial.

REFERÊNCIAS

ALECRIM, Emerson. **Facebook decide não excluir *deepfake* de Mark Zuckerberg no Instagram**. *Tecnoblog*, 12 jun. 2019. Disponível em: https://tecnoblog.net/noticias/facebook-vai-manter-*deepfake*-de-mark-zuckerberg/. Acesso em: 15 fev. 2025.

AMOROZO, Marcos. **Congresso tem pelo menos 46 projetos de lei para regulamentar do uso de inteligência artificial. CNN BRASIL, 2024**. Disponível em: https://www.cnnbrasil.com.br/politica/congresso-tem-pelo-menos-46-projetos-de-lei-para-regulamentar-do-uso-de-inteligencia-artificial/#goog_rewarded. Acesso em: 17 de fev. 2025.

AYYUB, R. **I Was The Victim Of A *Deepfake* Porn Plot Intended To Silence Me**. Huffpost. 2018. Disponível em: https://www.huffingtonpost.co.uk/entry/*deepfake*porn_uk_5bf2c126e4b0f32bd58ba316. Acesso em: 15 fev. 2025

BATTAGLIA, Rafael. **Afinal, o que são *deepfakes*?** 2020. Disponível em: https://super.abril.com.br/tecnologia/afinal-o-que-sao-*deepfakes*/ . Acesso: 22 set. 2023.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial - dos crimes contra a pessoa**. 17. ed. São Paulo: Saraiva, 2017.p. 314-317.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, RJ: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 fev. 2024

BRASIL. **Guia Ilustrado Contra as *Deepfakes***. Supremo Tribunal Federal; Data Privacy Brasil. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024. Disponível em: https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20*Deepfakes*_ebook%20(1).pdf. Acesso em: 17 de fev. 2025

BRASIL. **Lei nº 12.965 de 23 de abril de 2014: Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: Acesso em: 17 fev. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 fev. 2025.

BRASIL. **TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições**. TRIBUNAL SUPERIOR ELEITORAL (TSE). *Portal do TSE*, Brasília, DF, 28 fev. 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes. Acesso em: 17 fev. 2025.

CHESNEY, Robert; CITRON, Danielle Keats. **Deep fakes: a looming challenge for privacy, democracy, and national security.** California Law Review, v. 107, Texas: U of Texas Law - Public Law Research Paper No. 692, 2018, p. 6-16. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954. Acesso em: 15 fev. 2025.

CHINA. ***Criminal Law of the People's Republic of China*.** 1997. Disponível em: https://www.warnathgroup.com/wp-content/uploads/2015/03/China-Criminal-Code.pdf. Acesso em: 15 fev. 2025.

CHINA. **Administração do Ciberespaço da China Ministério da Indústria e Tecnologia da Informação da República Popular da China**, 25 de novembro de 2022. Disponível em: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm. Acesso em: 17 fev. 2025

CHINA'S BRIEFING NEWS. **China to Regulate Deep Synthesis (Deepfake) Technology from 2023**. Disponível em: <https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/>. Acesso em: 13 mar. 2025.

Correio Braziliense. (2018, 8 de março). **Fake news se espalham 70% mais rápido que notícias verdadeiras, aponta estudo do MIT.** Correio Braziliense. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2018/03/08/interna_tecnologia,664835/fake-news-se-espalham-70-mais-rapido-que-noticias-verdadeiras.shtml. Acesso em: 15 fev. 2025.

CRESWELL, J. W.; POTH, C. N. **Qualitative inquiry and research design: Choosing among five approaches**. [s.l.] Sage publications, 2016.

DAUER, Letícia. **Inteligência artificial: *deepfake* já foi usada em eleições pelo mundo.** UOL Confere, São Paulo, 3 mar. 2024. Disponível em: https://noticias.uol.com.br/confere/ultimas-noticias/2024/03/03/*deepfake*-uso-inteligencia-artificial-eleicoes-argentina-estados-unidos.htm. Acesso em: 17 fev. 2025

FAUSTINO, André. **Fake news e a liberdade de expressão nas redes sociais na sociedade da informação.** Dissertação de Mestrado (Mestrado em Direito da Sociedade da Informação) — Faculdades Metropolitanas Unidas, São Paulo, 2018. P. 106-110. Disponível em: http://arquivo.fmu.br/prodisc/mestradodir/af.pdf. Acesso em: 14 fev. 2024.

FINLAYSON-BROWN, Jane; NG, Susana. **China brings into force Regulations on the Administration of Deep Synthesis of Internet Technology addressing *deepfakes* and similar technologies.** A&O Shearman. 2023. Disponível em: <https://www.aoshearman.com/en/insights/ao-shearman-on-data/china-brings-into-force-regulations-on-the-administration-of-deep-synthesis-of-internet-technology>. Acesso em: 17 fev 2025.

GRECO, Rogério. **Curso de Direito Penal: parte especial. 2. Vol**. Impetus. Niterói, Rio de Janeiro. 2006. P. 455-460.

GUSTIN, M. B. DE S.; DIAS, M. T. F.; NICÁCIO, C. S. **(Re)pensando a Pesquisa Jurídica: Teoria e Prática**. 5. ed. São Paulo: Almedina, 2020.

HEMRAJANI, Asha. **China's new legislation on *deepfakes*: Should the rest of Asia follow suit?** THE DIPLOMAT. Disponível em: https://thediplomat.com/2023/03/chinas-new-legislation-on-*deepfakes*-should-the-rest-of-asia-follow-suit/ . Acesso em: 17 fev. 2025.

HOSTETTLER, Nicole**. Tongue-in-cheek: how Internet defamation laws of the United States & China are shaping global Internet speech**. Journal of High Technology Law, v. 9, p. 66, 2009. Disponível em: https://bpb-

use1.wpmucdn.com/sites.suffolk.edu/dist/5/1153/files/2018/02/HOSTETTLER_Tongue_in_Cheek-137eboq.pdf. Acesso em: 10 fev. 2025.

INTERESSE, Giulia. **China to Regulate Deep Synthesis (*Deepfake*) Technology Starting 2023**. China Briefing. 2023. Disponível em: https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/. Acesso em: 17 fev. 2025.

JIA, W. The Choice of Legislative Regulatory Model of Generative Artificial Intelligence in China. **China Legal Science**, v. 12, p. 133, 2024.

NUCCI, Guilherme de Souza. **Código Penal Comentado**, - 17º ed. Rio de Janeiro, RJ: Editora Forense, 2017. P. 687-688.

NOGUEIRA, Paulo Lúcio. **Em defesa da honra: doutrina, legislação e jurisprudência**. Imprenta: São Paulo, Saraiva, 1995. Descrição Física: p. 202

NUNES JÚNIOR, Vidal Serrano, e ARAUJO, Luiz Alberto David. **Curso de direito constitucional**. 3. ed. São Paulo: Saraiva, 1999. P. 97

Martins, J. **Metodologia da pesquisa científica**. Dowbis. 2017. P.22.

MEDON, Filipe. **O direito à imagem na era das *deepfakes***. Revista Brasileira de Direito Civil – RBD Civil: Belo Horizonte, v. 27, p. 251-277, jan/mar. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/438/447. Acesso em: 15 fev. 2025

MEZZAROBA, O.; MONTEIRO, C. S. **Manual de Metodologia da Pesquisa no Direito**. 7ª edição ed. São Paulo: Saraiva, 2017.

MOLINA, Adriano Cezar; BERENGUEL, Orlando Leonardo. ***Deepfake*: a evolução das fake news. Research, Society and Development**, v. 11, n. 6, 2022. Disponível em: http://dx.doi.org/10.33448/rsd-v11i6.29533. Acesso em: 17 fev. 2025

POSSA, Júlia. **China ganha lei para conter *deepfakes***. UOL. 2023. Disponível em: https://gizmodo.uol.com.br/china-ganha-lei-para-conter-*deepfakes*-entenda/. Acesso em: 17 fev. 2025.

RAMOS-ZAGA, F. Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial. **Derecho global. Estudios sobre derecho y justicia**, v. 9, n. 27, p. 359–387, 2024.

RIEGEL, Jeffrey. Confucius. In: ZALTA, Edward N. (Ed.). **The Stanford Encyclopedia of Philosophy. Stanford: Metaphysics Research Lab, Stanford University**, 2006. Disponível em: https://plato.stanford.edu/entries/confucius/. Acesso em: 11 fev. 2025.

ROBL FILHO, I. N.; MARRAFON, M. A.; MEDÓN, F. A inteligência artificial a serviço da desinformação: como as deepfakes e as redes automatizadas abalam a liberdade de ideias no

debate público e a democracia constitucional e deliberativa. **Economic Analysis of Law Review**, v. 13, n. 3, p. 32–47, 2022.

SENSITY TEAM. **Mapping the *Deepfake* Landscape. Sensity.** 2019. Disponível em: https://sensity.ai/blog/*deepfake*-detection/mapping-the-*deepfake*-landscape/ . Acesso em: 15 fev. 2025

SPAHN, Elizabeth. **As Soft as Tofu: Consumer Product Defamation on the Chinese Internet**. Vanderbilt Journal of Transnational Law, v. 39, n. 3, p. 865-879, 2006. Disponível em: https://scholarship.law.vanderbilt.edu/vjtl/vol39/iss3/4/ . Acesso em: 11 fev. 2025.