SIMPAR
Simpósio de Pesquisa, Extensão e Inovação do Paraná
Realização
IN2 Instituto Integrado de Ciência e Tecnologia
Centro Universitário Integrado
Núcleo de Empreendedorismo, Pesquisa e Extensão Integrado
Apoio
Fundação Araucária
Apoio ao Desenvolvimento Científico e Tecnológico do Paraná

# O uso indevido da inteligência artificial na produção de *deepfakes* e seus impactos sociais e jurídicos no Brasil

Acadêmico: Gabriel Kauê Repinácio, Direito, Centro Universitário Integrado, Brasil, grepinacio@gmail.com

Orientador: Professor Ramonn Luiz Silva Domingues, Direito, Centro Universitário Integrado, Brasil, ramonn.domingues@grupointegrado.br

**Resumo:** O estudo aborda o fenômeno das *deepfakes*, uma prática contemporânea que impôs ao Poder Judiciário e à sociedade o desafio de compreender, prevenir e responsabilizar as condutas relacionadas à manipulação digital produzida por inteligência artificial. A presente pesquisa analisa os impactos das *deepfakes* como uma nova maneira de cometer uma prática ilícita. Adotou-se uma abordagem qualitativa, de natureza exploratória e descritiva, com base em pesquisa bibliográfica, documental e jurisprudencial, tendo como principais referências a Constituição Federal de 1988, o Código Penal e a doutrina contemporânea. O objetivo é demonstrar os reflexos jurídicos e sociais da utilização dessa tecnologia. A rápida e indetectável proliferação desses conteúdos digitais evidencia a urgência em promover uma tutela jurídica efetiva que consiga mitigar os danos concretos e irreversíveis à reputação. Conclui-se, portanto, pela urgência de um Marco Regulatório específico para a Inteligência Artificial (Projeto de Lei 2338/2023) que estabeleça mecanismos de identificação, responsabilização e assegure o necessário equilíbrio entre a proteção dos direitos fundamentais e o estímulo à inovação tecnológica.

**Palavras-chave:** Inteligência Artificial. *Deepfake*. Lei. Direitos da Personalidade. Dignidade da Pessoa Humana.

**Abstract:** This study addresses the phenomenon of deepfakes, a contemporary practice that has presented the Judiciary and society with the challenge of understanding, preventing, and holding accountable those responsible for conduct related to digital manipulation produced by artificial intelligence. This research analyzes the impacts of deepfakes as a new way of committing an illicit act. A qualitative, exploratory, and descriptive approach was adopted, based on bibliographic, documentary, and jurisprudential research, with the 1988 Federal Constitution, the Penal Code, and contemporary doctrine as the main references. The objective is to demonstrate the legal and social repercussions of the use of this technology. The rapid and undetectable proliferation of this digital content highlights the urgency of promoting effective legal protection that can mitigate concrete and irreversible damage to reputation. It is concluded, therefore, that there is an urgent need for a specific Regulatory Framework for Artificial Intelligence (Bill 2338/2023) that establishes mechanisms for identification and accountability, and ensures the necessary balance between the protection of fundamental rights and the encouragement of technological innovation.

**Keywords:** Artificial Intelligence. *Deepfake*. Law. Personality Rights. Human Dignity.

## INTRODUÇÃO

O presente estudo estrutura-se em três capítulos: o primeiro analisa o conceito e a evolução das *deepfakes*, seus impactos sociais e jurídicos; o segundo examina a proteção dos direitos da personalidade e a insuficiência do ordenamento

jurídico brasileiro diante dessa nova forma de manipulação digital; e o terceiro apresenta as alternativas estatais e institucionais no Brasil e o comparativo com o cenário internacional, propondo reflexões sobre a necessidade de adaptação do Direito Penal e Constitucional à realidade tecnológica contemporânea.

Tal prática, que inicialmente surgiu como uma inovação tecnológica voltada ao entretenimento, evoluiu exponencialmente para um cenário de preocupante potencial ofensivo, atingindo direitos fundamentais da personalidade e gerando novos desafios ao ordenamento jurídico brasileiro.

A partir da expansão da inteligência artificial generativa, tornou-se cada vez mais difícil distinguir o que é real do que é artificialmente produzido. Essa transformação trouxe implicações diretas à proteção da honra, da imagem e da dignidade da pessoa humana, valores consagrados nos artigos 1º, inciso III, e 5º, inciso X, da Constituição Federal de 1988.

Assim, tanto a sociedade quanto o Poder Judiciário, que até então, em total desconhecimento legislativo das novas práticas, é chamado a enfrentar uma nova categoria de ofensas: aquelas que, ainda que digitais e inexistentes de certa forma, produzem efeitos concretos e irreversíveis sobre a reputação, a privacidade e as finanças das pessoas.

A problemática que orienta este estudo consiste em compreender como o uso indevido da inteligência artificial na produção de *deepfakes* compromete a autenticidade da realidade digital e desafia a efetividade da tutela jurídica dos direitos da personalidade no Brasil.

Diante disso, busca-se analisar as lacunas normativas e os limites da legislação penal vigente, considerando que, apesar de avanços pontuais como a recente Lei nº 15.123/2025, que agrava penas quando comprovado o uso de *deepfakes* em condutas criminosas, o sistema jurídico brasileiro ainda se mostra insuficiente, até o momento, para conter e reprimir o impacto social e moral dessas práticas.

Por fim, pretende-se demonstrar que o fenômeno das *deepfakes* não é apenas uma consequência do avanço tecnológico, mas um reflexo da crise de autenticidade da era digital uma crise que exige do Direito respostas urgentes para garantir a proteção da verdade, da imagem e da dignidade humana.

## MÉTODO

O presente trabalho utiliza o método de abordagem dedutivo, partindo de premissas gerais acerca do avanço tecnológico e de seus reflexos no campo jurídico, para então analisar as consequências específicas do uso indevido da inteligência artificial na produção de *deepfakes*.

A abordagem de pesquisa é qualitativa, de natureza exploratória e descritiva, voltada à compreensão e análise crítica dos efeitos jurídicos e sociais decorrentes da evolução exponencial da inteligência artificial contemporânea, fundamentada em pesquisa bibliográfica, documental e jurisprudencial.

O estudo foi aprofundado por meio de pesquisa bibliográfica, documental e comparativa, abrangendo fontes normativas e documentais, como a Constituição

Federal de 1988 (em especial, os artigos 1º, inciso III, e 5º, inciso X, que tratam da dignidade humana e dos direitos da personalidade), o Código Penal Brasileiro de 1940, a recente Lei nº 15.123/2025, e de projetos de lei em tramitação, como o PL 2338/23 (Marco da Inteligência Artificial), que versa sobre o uso mal-intencionado de IAs.

Também foi utilizado Doutrina e Artigos Científicos abordando a temática sob a ótica do Direito Penal, Constitucional e da proteção dos direitos da personalidade. A doutrina de referência oferece base teórica para a análise crítica da necessidade de adequação do Direito às novas formas de manipulação digital, visto que os desafios contemporâneo inerentes a evolução da tecnologia estão sendo tipificados através de uma Lei que está em vigor desde 1940.

Por fim, a pesquisa comparativa analisou experiências internacionais, como o Regulamento (UE) 2024/1689 (*AI Act*) e a Convenção de Budapeste, com o objetivo de avaliar modelos regulatórios aplicáveis ao contexto brasileiro. Essa abordagem permite não apenas compreender a dimensão global do fenômeno das *deepfakes*, mas também propor reflexões críticas sobre o papel do Judiciário brasileiro na busca da preservação da imagem, da honra e da dignidade humana em meio à transformação tecnológica contemporânea.

## RESULTADOS E DISCUSSÃO

### 1 A *DEEPFAKE* COMO COROLÁRIO DA INTELIGÊNCIA ARTIFICIAL: CONCEITO E SUAS CONSEQUÊNCIAS NA SOCIEDADE

Em 2017, um usuário do *Reddit*[1], com o pseudônimo de "*deepfake"* divulgou vídeos falsos nos quais atrizes de *Hollywood* onde tiveram seus rostos inseridos em vídeos de conteúdo adulto, vídeos esses que jamais existiram e até então apontaram como mera montagem.

Nesse segmento, a tecnologia do *deepfake* usa o algoritmo *Deep Learning* (aprendizagem profunda) na elaboração de conteúdos falsos, criando situações embaraçosas e disseminando conteúdo e informações falsas.

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

Para Lalla; Mitrani; Harned (2022), *deepfake* se refere a uma técnica baseada em inteligência artificial capaz de sintetizar áudios e vídeos, sobrepondo as feições de uma pessoa ao corpo de outra e/ou manipulando sons para produzir uma experiência humana realística.

Já Spencer (2019) define as *deepfakes* como identidades falsas criadas com o *deep learning* (aprendizagem profunda, por meio de uso maciço de dados),

[1]Reddit é uma comunidade que permite que os usuários interajam por meio de postagens anônimas e comentários. Os usuários se agrupam em comunidades (subreddits) que escolhem por serem mais alinhadas com seus tópicos de interesse (Lima; Pagano; Silva, 2024).

técnica que combina e sobrepõe imagens e vídeos preexistentes para transformá-los em conteúdos “originais”.

No cenário internacional, Maras; Alexandrou (2018) ressaltam que os vídeos *deepfake* são produtos de aplicações de inteligência artificial que mesclam, substituem e sobrepõem imagens e videoclipes, criando conteúdos falsos que aparentam autenticidade. Os autores alertam que o principal problema dessas produções é o potencial de gerar conteúdo explícito sem o consentimento dos envolvidos, corroendo a confiança nas evidências em vídeo e afetando negativamente seu valor probatório em tribunais.

Nesta esteira, fica transparente que o fenômeno das *deepfakes* ultrapassa um mero acessório das Inteligências Artificiais, tratando-se praticamente de um instrumento quase independente das Inteligências Artificiais, que quando o usuário, imbuído de má-fé e intenção de praticar um delito criminoso a um terceiro, pode se tornar uma grave ameaça à integridade moral e à imagem das pessoas, inaugurando uma nova fronteira de riscos jurídicos e sociais. A principal característica desse fenômeno consiste em sua acessibilidade e praticidade. Nunca um indivíduo sem conhecimento técnico especializado pôde produzir conteúdos digitais de alto realismo ou competir com profissionais da área.

## 1.2 A repercussão social e jurídica do uso indevido das *deepfakes*

Antes mesmo do surgimento das tecnologias de manipulação digital, o ordenamento jurídico brasileiro já previa a proteção da imagem e da dignidade humana como direitos fundamentais.

A Constituição Federal de 1988 garante, no art. 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Não obstante, a Constituição também resguarda, de forma categórica, no art. 1º, inciso III, a dignidade da pessoa humana como fundamento do Estado Democrático de Direito.

Nas palavras de Camargo (2016), o Estado, nessas condições, precisa estar presente para garantir o cumprimento do princípio da dignidade da pessoa humana, no sentido de garantir o mínimo existencial a todos e a liberdade do indivíduo, é o dever básico de qualquer Estado, pois todos são iguais perante a Lei.

Affonso (2021), salienta que, embora o Código Civil contemple a proteção da imagem como um bem jurídico tutelado, os mecanismos de reparação ainda se mostram ineficazes para lidar com os efeitos ampliados da exposição digital, como a replicação em larga escala e a dificuldade de remoção definitiva do conteúdo.

Agora, trazendo um pouco da relação prática, as deepfakes já produziram efeitos prejudiciais catastróficos na sociedade. Com o avanço e melhoria da Perfomance das Inteligências Artificias, hoje dificilmente qualquer usuário comum das redes sociais conseguem distinguir um vídeo real e um vídeo produzido por Inteligência Artificial.

Em termos sociais, os efeitos da manipulação audiovisual são alarmantes. A deputada Jandira Feghali, autora da Lei nº 15.123/2025 e de projetos voltados à

criminalização de conteúdos *deepfake*, destacou o aumento de 96% nos casos de pornografia *deepfake* e de 900% nos casos de *deepfakes* de violência, sendo as mulheres as principais vítimas dessas práticas.

A senadora Daniella Ribeiro (PSD-PB), relatora da Lei nº 15.123/2025 acrescenta que a evolução tecnológica tem potencializado novas formas de agressão, sobretudo contra mulheres, violando sua dignidade e autoestima.

Nesse mesmo segmento de números significativos, foi realizada uma pesquisa pelo Comitê Gestor da Internet no Brasil, sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros, divulgada em 2023 pelo próprio Comitê, no qual constou como resultado a significativa parcela de 37% das pessoas que acessam a internet apenas pelo celular checam as informações recebidas (CGI.br 2023).

É dizer que, além de haver uma grande parcela de vítimas das *deepfakes*, ainda assim para agravar a situação, parte dos usuários sequer chegam as informações. Isso gera todo um cenário extremamente prejudicial, virando um efeito cascata, com a praticidade das *deepfakes* cada vez mais tem-se vítimas e plateia.

Nesse sentido, desdobrando apenas para a parte jurídica das *deepfakes*, quando o vídeo é feito, o dano já está consolidado. O doutrinador Bittar (2004), já interpretou no sentido que:

> Qualificam-se como morais os danos em razão da esfera da subjetividade, ou do plano valorativo da pessoa na sociedade, em que repercute o fato violador, havendo-se como tais aqueles que atingem os aspectos mais íntimos da personalidade humana (o da intimidade e da consideração pessoal), ou o da própria violação da pessoa no meio em que vive e atua (o da reputação ou da consideração social).

Essa pesquisa evidenciou que o uso indevido da inteligência artificial impacta não apenas os direitos individuais, mas também o equilíbrio social e a confiança pública nas relações humanas e institucionais.

### 1.3 As respostas do Estado e o crescimento exponencial das *deepfakes*

O poder público tem buscado, ainda que de forma urgente, reagir à proliferação de conteúdos manipulados por inteligência artificial. Um exemplo é o guia ilustrado contra as deepfakes, elaborado pelo Supremo Tribunal Federal sob a coordenação e redação do ministro e até então presidente do STF, Luís Roberto Barroso (2024), que busca conscientizar a sociedade sobre os riscos da desinformação digital e os limites éticos do uso da tecnologia.

Outro dado que importa destaque é a pesquisa divulgada pelo Ministério Público do Estado de Mato Grosso, que relatou um aumento de 822% nas fraudes utilizando *deepfake* entre o primeiro trimestre de 2023 e o mesmo período de 2024, conforme pesquisa da empresa de verificação de identidade Sumsub.

Em meio a esse grave cenário no âmbito da proteção das mulheres, que são o principal foco dos agentes praticantes das *deepfakes* foi sancionada a Lei nº 15.123/2025 que introduziu o artigo 147-B no Código Penal, estabelecendo causa

de aumento de pena para os crimes de ameaça e violência praticados com o uso de tecnologias de inteligência artificial.

Essa lei demonstra que o Poder Legislativo juntamente com a necessidade de punir pelo Poder Judiciário implica na representatividade em adequar o ordenamento jurídico brasileiro à realidade das manipulações digitais, ao reconhecer que a utilização de recursos algorítmicos potencializa a gravidade da conduta e amplia o alcance do dano.

Tanto uma alternativa de prevenção proferida pela Suprema Corte do país, quanto os dados coletados do Ministério Público apontam e de demonstram a vulnerabilidade da sociedade e o pequeno alcance, até o momento, do Estado em proteger a privacidade e imagem do indivíduo.

Esses números demonstram que o fenômeno da *deepfake* não se limita ao campo do entretenimento, mas alcançam dimensões de segurança pública, política, econômica e jurídica. A crescente utilização dessa tecnologia em golpes, difamações e manipulação de informações comprova a urgência de medidas legislativas e penais capazes de conter seus efeitos danosos.

Pelo comportamento da mídia, diante de uma situação não comprovada, promoveu a consequente execração pública das pessoas envolvidas, onde a sociedade, com base nas informações difundidas nos meios de comunicação, julgou os acusados antes da devida apreciação do caso pelo judiciário. As sequelas emocionais dos envolvidos, com certeza, são insanáveis. (SILVA, 2006)

Esse fenômeno representa uma das manifestações mais complexas da era digital, unindo o avanço tecnológico à fragilidade da legislação atual tradicional. Sua rápida proliferação desafia o Direito a repensar os mecanismos de proteção da imagem, da honra e da dignidade da pessoa humana, bens jurídicos diretamente afetados pela manipulação audiovisual.

Todo tipo de dano por ser causado pela *deepfake*, seja a uma unidade, ao coletivo, a uma pessoa anônima e até mesmo a algum político.

Em tese, uma *deepfake*, respeitando os limites legais, pode ser usada como um instrumento criativo para expor seus ideais, porém, existe uma linha tênue entre se expressar manifestamente e cometer um crime.

A vasta acessibilidade às mídias digitais tem-se que é preocupante o uso de redes sociais em campanhas eleitorais por partidos, candidatos e indivíduos em geral, eis que acabam difundindo com mais facilidade as notícias falsas, comprometendo o processo (FILAGRANA, 2021, P. 49).

A atuação estatal ainda se mostra frágil diante da dimensão do problema. Embora iniciativas legislativas e orientações institucionais estejam em andamento, o crescimento exponencial das ocorrências revela que as medidas atuais são insuficientes para conter o uso ilícito dessa tecnologia.

Em outras palavras, a *deepfake* evidencia o descompasso entre o progresso tecnológico e a efetividade da proteção jurídica, demonstrando a necessidade de uma tutela penal específica e de políticas públicas que garantam a segurança digital e a preservação dos direitos da personalidade.

Visando uma alternativa para reprimir tais contextos, Jardim (2024) defende a ampliação das competências da administração pública para fiscalizar plataformas e exigir protocolos de detecção automática e remoção célere de conteúdos manipulados.

Entretanto, Fernandes (2024) indica que o paradoxo entre a proteção da privacidade e o desenvolvimento da inteligência artificial escancara uma lacuna normativa que compromete o controle sobre a disseminação de informações falsas.

Restante assim, de forma evidente, o impacto jurídico que as *deepfakes* vem causando na sociedade.

## 2 DA VULNERABILIDADE DOS DIREITOS DA PERSONALIDADE NO CONTEXTO DAS DEEPFAKES E AS ALTERNATIVAS VIGENTES DO PODER JUDICIÁRIO.

A disseminação das tecnologias de inteligência artificial, em especial as *deepfakes*, inaugurou um cenário de intensa vulnerabilidade aos direitos da personalidade, notadamente à imagem, honra, privacidade e dignidade da pessoa humana.

Em sede de julgamento, a época, o Ministro do STJ Raul Araújo (2012), na sua relatoria acerca do julgamento de um Recurso Especial sobre o uso indevido da imagem a mais de 10 anos atrás já pontuava que a ofensa ao direito à imagem materializa-se com a mera utilização da imagem sem autorização, ainda que não tenha caráter vexatório ou que não viole a honra ou a intimidade da pessoa, e desde que o conteúdo exibido seja capaz de individualizar o ofendido.

O direito à privacidade é um dos direitos mais impactados com as transformações tecnológicas, sociais e políticas, atualmente vivenciadas. De uma origem muito intimista, qual seja, o direito de estar só ou de não ser perturbado, ampliou-se para um conjunto de faculdades que dizem respeito a esferas existenciais e patrimoniais, em espaços físicos e virtuais. (Bolesina e Gervasoni, 2022)

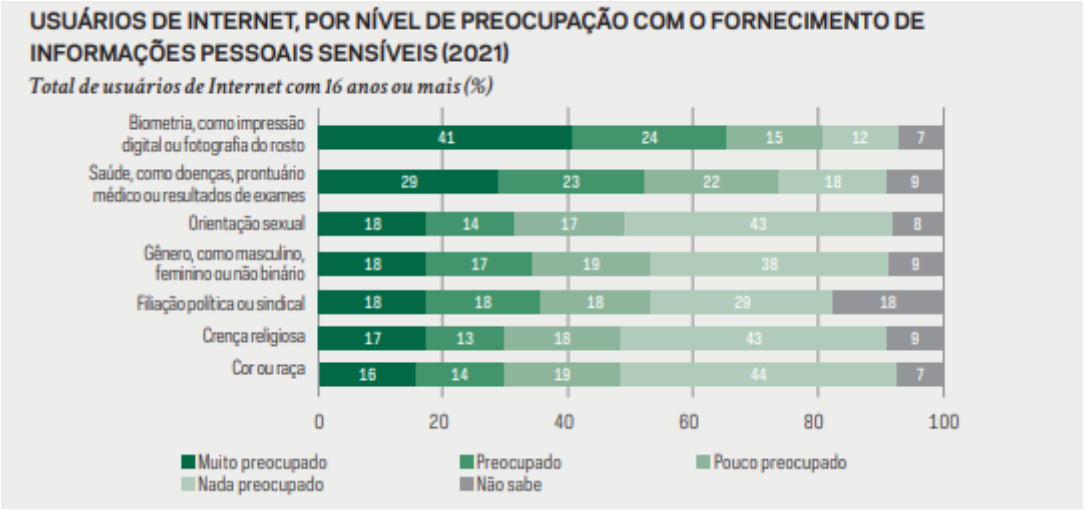
O Ministro do STJ, Ricardo Villas Bôas Cueva (2018), expõe que as *fakes news* têm potencial destrutivo e podem criar uma verdadeira crise na democracia, ao estimular elevada volatilidade no eleitorado.

Nesse mesmo sentido, Robles-Lessa; Cabral; Silvestre (2020) advertem que os riscos sociais e jurídicos das *deepfakes* transcendem a violação da imagem: atingem a dignidade humana, ao expor pessoas à difamação, extorsão e constrangimento público em escala global. No ambiente do ciberespaço, onde os conteúdos circulam com alta velocidade e difícil rastreabilidade, a reparação torna-se quase impossível.

Destacam também que a inteligência artificial utilizada nos deepfakes atua diretamente na desinformação global, reproduzindo informações falsas, enganosas, descontextualizadas e projetadas com o intuito de causar malfeitorias à coletividade, causando um colapso de desconfiança a tudo que é publicado na rede mundial de computadores (ROBLES-LESSA; CABRAL E SILVESTRE, 2020).

Corroborando com a iminência da desinformação global, foi feita uma pesquisa em 2021 acerca dos usuários da internet e o nível de preocupação com o fornecimento de informações pessoais sensíveis:

Gráfico 1 Usuários de Internet, por nível de preocupação com o fornecimento de informações pessoais sensíveis (2021)




Fonte: NIC.br; CGI.br. Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil – 2021. São Paulo: Comitê Gestor da Internet no Brasil, 2022.

Nesse contexto, a facilidade da propagação das *deepfakes* fica muito mais simples, o agente mal-intencionado não tem dificuldade em conseguir dados e a vítima não tem receio de se expor perante os agentes.

Como já demonstrado, o impacto das *deepfakes* no cenário brasileiro ultrapassa o campo teórico e atinge diretamente a esfera política, social e moral dos indivíduos, em outras palavras, qualquer pessoa pode ser uma vítima da *deepfake* a qualquer momento em qualquer contexto.

Um exemplo emblemático é o caso da prefeita e candidata à reeleição ao cargo de prefeita de Bauru (SP), Suéllen Rosim, foi vítima de uma *deepfake* durante o período eleitoral de 2024. O vídeo, amplamente disseminado nas redes sociais, simulava declarações falsas e comprometedoras, manipuladas por inteligência artificial para imitar sua voz e aparência com alto grau de realismo. (CartaCapital, 2024)

A situação rapidamente ganhou repercussão nacional, porém, o prejuízo já estava concretizado. Segundo reportagem da CartaCapital, o vídeo enganou grande parte do público e de seus próprios eleitores antes de ser desmentido.

Ainda voltado para o contexto da vulnerabilidade da mulher e a violação do direito de imagem, a empresa *Sensity* noticiou que inteligências artificiais já criaram 'nudes' falsos de mais de 100 mil mulheres compartilhados em redes no ano de 2020.

Nenhum integrante da sociedade está imune a se tornar vítima dessa conduta criminosa. A periculosidade de um instrumento tão simples capaz de causar danos significativos é evidente. Contudo, até o momento, a legislação ainda não definiu com precisão a responsabilidade dos envolvidos. Em outras palavras,

as *deepfakes* permanecem em uma zona de incerteza jurídica, sem um marco legislativo específico que discipline a penalização dos responsáveis.

Em apontamento anterior, já foi exposto sobre o entendimento do Ministro Ricardo Villas Bôas Cueva acerca da utilização de tecnologias como forma de enfrentamento às *fake news*.

Segundo o ministro, o Marco Civil da Internet (Lei n. 12.965/4) encontra-se defasado no tocante ao combate às notícias falsas, sendo uma possível alternativa a criação de um algoritmo capaz de identificar conteúdos inverídicos. Em outras palavras, regulamentar, de forma estatal, as Inteligências Artificiais.

Todavia, o próprio Cueva reconhece que tal medida poderia gerar novas controvérsias, sobretudo quanto à definição dos parâmetros que distinguiriam o verdadeiro do falso (CUEVA, 2018).

Nessa linha de reflexão, Mendonça e Rodrigues (2018) destacam que a proposta de criação de um algoritmo para detectar *fake news* suscita questionamentos éticos e jurídicos relevantes, como:

O controle da “caixa-preta” do algoritmo e a definição de quem determinaria os critérios de veracidade da informação seriam de uma única só pessoa?

A inteligência Artificial, em outras palavras, deixaria de se tornar única, o seu principal requisito que seria a espontaneidade e “livre arbítrio” seria regulamentado e limitado.

Para Rodrigues (2024), as alternativas para reprimir as *deepfakes* estão em espécies de Auditoria Algoritmia, Educação digital ou até mesmo Mecanismos de supervisão.

Uma alternativa para resolver problemas contemporâneos é analisar como o Direito Penal se portou aos problemas similares do passado, nesse segmento, antes mesmo das *deepfakes,* já existiam os conteúdos digitais alterados, nesse sentido, Zaffaroni (2013) pontua o seguinte:

> A criminologia midiática sempre existiu e sempre apela a uma criação da realidade através de informação, subinformação e desinformação em convergência com preconceitos e crenças, baseada em uma etiologia criminal simplista, assentada na causalidade mágica. Esclarecemos que o mágico não é a vingança, e sim a ideia da causalidade especial que se usa para canalizá-la contra determinados grupos humanos, o que, nos termos da tese de Girard, os converte em bodes expiatórios.

Em palavrado do doutrinador, o sistema penal é autofágico. Ele se alimenta de si mesmo (LOPES JR., 2010, p. 17). Ou seja, um ponto positivo para o fenômeno das *deepfakes* é que, de acordo com a história do Direito Penal, existe solução.

O que se alardeia, ainda, que muito de nossa legislação penal é irracional, portanto, obsoleta, tornando o público moralmente indignado e atenua suas emoções em vinganças localizadas (SILVA, 2006).

Diante de todo esse panorama, verifica-se que o uso indevido das *deepfakes* agride diretamente os direitos da personalidade, ao explorar a imagem e a identidade das pessoas sem consentimento e sem limites éticos ou jurídicos claros.

A proteção à privacidade e à honra, embora assegurada constitucionalmente, mostra-se fragilizada diante das novas dinâmicas digitais, em que a manipulação da realidade é quase indetectável.

## 2.1 A regulação global da inteligência artificial na regulação das Inteligências Artificiais

A consolidação da chamada Quarta Revolução Industrial, segundo Schwab (2019, p. 4-5), caracteriza-se pela fusão de tecnologias físicas, digitais e biológicas, transformando profundamente as relações sociais e jurídicas.

A Lei 12.965/2014 (Marco Civil da Internet) define princípios, garantias, direitos e deveres para a utilização da internet no Brasil. Nesse mesmo âmbito de proteção digital já existente na jurisdição digital, A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 por seu lado, atua na imposição de obrigações de consentimento, transparência e responsabilização para os controladores de dados, conferindo também ao cidadão direitos como os de acessar, corrigir e excluir seus dados.

Podemos citar ainda as Lei n° 12.735/2012, n° 12.737/2012, que abordam a tecnologia por meio de aspectos como o uso de ferramentas de interação e comunicação num arcabouço de proteção principiológica ao usuário e ao provedor, como também o tratamento de dados pessoais e a divulgação de cenas criminosas por meios digitais (SIQUEIRA, 2019).

Infelizmente, pela falta de previsibilidade expressa e específica sobre as *deepfakes* no ordenamento vigente, muitos operadores do direito consideram a aplicação de diversos instrumentos citados anteriormente como inadequada, o que penas evidencia a necessidade de atualizações e mudanças (SIQUEIRA, 2019).

Partindo da jurisdição nacional e corroborando com a colaboração internacional, a Convenção de Budapeste traz relevantes novidades sobre cooperação jurídica internacional para obtenção de provas digitais (arts. 23 a 35), com o potencial de tornar mais eficiente a obtenção de provas entre o Brasil e outros 67 Estados. (MURATA E TORRES, 2023, P.14).

Trazendo uma relação de contexto internacional, vislumbrando algum tipo de exemplo jurídico sobre o combate as *deepfakes* num contexto global, A Convenção de Budapeste pode ser um importante referencial.

A Convenção de Budapeste foi incorporada no ordenamento jurídico brasileiro num momento em que diversos temas que tocam a criminalidade cibernética estão em voga, como o vazamento de dados, os golpes informáticos e o uso da internet para a disseminação das *fake News* (MURATA E TORRES, 2023, P.14).

Ainda no contexto de preencher as lacunas deste crime contemporâneo, os crimes cibernéticos incluem todos os crimes praticados na internet como pornografia infantil, violação à segurança de redes, violações de direitos autorais e conexos, assim como fraudes relativas a dados e sistemas (FERRARI; SENNA, 2020).

Nesse mesmo sentido, para efeito de comparação com a atual possibilidade jurídica brasileira de combate as *deepfakes*, o Regulamento (UE) 2024/1689 (*AI Act*) estabelecendo regras harmonizadas sobre Inteligência Artificial na União Europeia com abordagem baseada em risco e integrações com a legislação do mercado interno.

O art. 1º do *AI Act* fixa seus objetivos: melhorar o funcionamento do mercado interno e promover uma IA centrada no ser humano e de confiança, assegurando alto nível de proteção à saúde, segurança e direitos fundamentais.

A União Europeia avançou novamente com o *AI Act* (2023), antes de entrar em vigor a definição que define a IA como um sistema baseado em máquinas com autonomia variável, capaz de inferir resultados e influenciar ambientes (UNIÃO EUROPEIA, 2023, p. 10).

Esse marco regula a IA conforme níveis de risco e obriga a identificação explícita de conteúdos sintéticos, especialmente *deepfakes*, impondo transparência como princípio ético e jurídico. Trata-se de uma abordagem preventiva, orientada à preservação da dignidade e da autodeterminação informativa dos cidadãos.

No Brasil, embora exista a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), sua aplicação direta aos sistemas de IA ainda é limitada. Em outras palavras, a defesa que a aplicação analógica da LGPD pode mitigar riscos à privacidade, uma vez que a legislação atual não contempla especificidades da IA generativa.

Atualmente, sistemas de IA em utilização no Brasil não possuem nenhuma regulamentação específica; essa lacuna legislativa ocorre em razão da própria morosidade do processo legislativo e da ausência de interesse/prioridade do legislador. (BELEZA, 2021, P. 35).

Não obstante, o limite das funções das Inteligências Artificiais mais sofisticadas é a criatividade do usuário, corroborando com o exposto, Neves e Almeida (2024, p. 120), categoricamente trazem a urgência legislativa como um costume popular que deve ser atendido.

> Nas sociedades democráticas e pluralistas, é importante primeiro prestar atenção aos seus valores identitários e construir um consenso ético inclusivo e amplo, como base legitimadora para as normas legais a serem formuladas posteriormente pela Lei.

Na mesma linha, o Parlamento Europeu (2017), em seu relatório sobre normas civis de robótica, enfatiza que a autonomia das máquinas deve ser acompanhada de deveres correlatos de transparência e proteção de dados pessoais.

Por fim, autores como Monteiro (2018, p. 21) e Tacca e Rocha (2018, p. 21) destacam que o direito digital deve ser compreendido como um campo de integração entre segurança, privacidade e inovação, onde o desafio maior é manter o equilíbrio entre liberdade tecnológica e proteção da dignidade humana.

Dessa forma, tanto no Brasil quanto ao redor do mundo, os países enfrentam problemas enraizados na sociedade, a regularização e as medidas de segurança para serem utilizadas nas IAs sempre se resultam em dois pontos:

O primeiro versa sobre a necessidade e urgência da sociedade e o poder público se protegerem dos efeitos devastadores das *deepfakes*, fenômeno que está em alta no Brasil justamente pela falta de medida de segurança eficaz contra a disseminação.

O atual secretário-executivo do Ministério da Fazenda, Dario Durigan (2025), em debate na Comissão Especial sobre Inteligência Artificial, destacou a importância dessa regulação ao afirmar que é necessário encontrar os caminhos, como temos feito, para abrir um novo ciclo de desenvolvimento para o país, que tenha por premissa a responsabilidade fiscal, o compromisso social, ecológico e com o desenvolvimento digital, com a pessoa no centro do debate.

Já em sentido oposto, o outro ponto totalmente se sobrepõe em via oposta, expondo mais uma vertente sustentada pelo dogma de que controlar excessivamente a Inteligência Artificial seria o mesmo que anular sua essência autônoma e independente.

Nessa visão, ao restringir sua capacidade de agir de forma criativa e autorreferente, a IA deixaria de cumprir seu verdadeiro propósito ser uma criação humana capaz de pensar, interpretar e raciocinar de modo semelhante ao próprio homem com certa autonomia.

## 2.2 Dos avanços internacionais e dos desafios brasileiros na criação de protocolos de segurança para a inteligência artificial

As Inteligências Artificiais consolidaram-se como um dos principais setores da transformação digital contemporânea, em outras palavras, um divisor de águas entre antes e depois como a tecnologia funcionava sem a referida tecnologia.

No Brasil, conforme apontam Kubota e Rosa (2024), observa-se um processo de expansão em larga escala, no qual coexistem avanços significativos em pesquisa e lacunas estruturais na regulamentação e governança pública.

Dessa forma, o panorama internacional demonstra que a regulação da inteligência artificial e das *deepfakes* exige uma abordagem transnacional, ética e interdisciplinar, baseada em princípios comuns de responsabilidade, transparência e controle informacional.

Em contraste, países do G7, como o Reino Unido e o Japão, adotam políticas de estímulo baseadas em *sandboxes* regulatórias, as quais favorecem a integração entre desenvolvimento tecnológico e segurança jurídica.

No Brasil, tal dispositivo de segurança ainda não é utilizado, sobretudo no setor público, onde os índices de adoção variam de forma acentuada entre Poderes e entes federativos.

Como se percebe logo no início de sua obra, Cristie Ford (2017) parte da premissa de que a regulação tem por finalidade ordenar as relações sociais e econômicas, mas que sua concepção estática isto é, baseada em estruturas fixas e uniformes gera duas disfuncionalidades fundamentais: a desatualização, quando as normas não acompanham a velocidade das inovações, e a descontextualização, quando se aplicam regramentos uniformes a contextos distintos, desconsiderando as complexidades e especificidades setoriais.

Diante disso, Ford (2017) propõe uma regulação dinâmica e contextualizada, capaz de responder de modo flexível às transformações tecnológicas e institucionais, vinculando as ferramentas regulatórias aos valores sociais que pretendem proteger, e não apenas à sua função técnica.

Essa interpretação é elencada por Fenner Stewart (2019), ao afirmar que Ford Redefine a regulação flexível como uma forma de ação jurídica que se apoia em forças não legais como normas comunitárias, moralidade individual e forças de mercado, apresentando-a como um meio de superar as falhas de modelos rígidos e descontextualizados.

O autor destaca que tais falhas decorreram da tentativa de aplicar teorias estáticas a práticas dinâmicas, resultando em ineficácia e descompasso com a realidade social.

No mesmo sentido, Lazcano (2019) observa que Ford (2017) evidencia a diferença entre reconhecer que os legisladores antecipam certo nível de mudança e tentar implementar esforços regulatórios capazes de reagir e se adaptar a tendências evolutivas cada vez mais rápidas e complexas.

Assim, ambos os comentadores reforçam que a regulação deve ser continuamente adaptável, sob pena de tornar-se obsoleta e desconectada do contexto histórico e tecnológico a que se destina.

Conforme observam Kubota e Lins (2022), os órgãos públicos brasileiros ainda não possuem sistemas digitais que se comuniquem entre si, nem uma coordenação central capaz de integrar essas iniciativas. Cada instituição costuma adotar suas próprias plataformas e métodos, o que dificulta o compartilhamento de informações e reduz a eficiência das ações tecnológicas. Essa falta de integração, segundo os autores, acaba atrasando a modernização administrativa e o uso mais inteligente da tecnologia no setor público.

O principal desafio brasileiro para alcançar a regulamentação de forma “livre” consistiria em equilibrar regulação, ética e inovação tecnológica atrelado juntamente ao livre acesso de cada cidadão a IA.

Conforme Filgueiras (2022), a governança de IA na América Latina é fragmentada e vulnerável ao poder político, carecendo de instâncias técnicas independentes. Já Radu (2021) acrescenta que a ausência de estratégias coerentes amplifica desigualdades tecnológicas e dependências externas.

Nessa linha de estudos, a regulamentação ou até mesmo um consenso do uso das Inteligências Artificiais dependem de dois polos opostos concordar em abrir mão, tanto via que defende a liberdade absoluta quanto a via que defende a limitação para um bem maior.

Rikap e Lundvall (2021) alertam que a corrida global pela inovação tende a reproduzir hierarquias entre países produtores e consumidores de tecnologia, reforçando a necessidade de um modelo nacional de regulação que garanta autonomia tecnológica, proteção de direitos fundamentais e competitividade internacional.

Estudos recentes do NIC.br indicam que o Judiciário, o Legislativo e o Ministério Público do Brasil superam 40% de uso de IA em processos internos, ao

passo que o Poder Executivo federal apresenta níveis inferiores, evidenciando falta de interoperabilidade e de diretrizes unificadas.

Conforme Kubota e Lins (2024), essa disparidade decorre da ausência de planejamento integrado e de políticas permanentes de inovação tecnológica no serviço público.

Em um cenário em que já caminha para a realidade, o Brasil ficando para trás no quesito de pontuar os limites da Inteligência Artificial, restará, conforme estudos, seguir métricas de sistemas regularizadores já implantados em outros países.

Filgueiras (2022) já destacou que a política de IA na região tende a reproduzir modelos estrangeiros sem adequada contextualização, o que perpetua dependências tecnológicas e reduz a autonomia.

No quesito de desenvolvimento regulatório e medida de segurança, Japão e Reino Unido desenvolveram diretrizes éticas centradas no conceito de "IA humanocêntrica" (*human-centric AI*) e adotaram modelos regulatórios pró-inovação.

Já no contexto brasileiro permanece limitado à discussão legislativa dos Projetos de Lei nº 21/2020 e nº 2.338/2023, carecendo de movimentação do Poder Executivo.

Para Kubota e Rosa (2024), a atuação executiva deveria priorizar a promoção da inovação responsável, a proteção do consumidor e o fortalecimento da competitividade global, seguindo as recomendações da *OCDE* sobre a "*Regulatory Sandboxes in Artificial Intelligence"*.

O principal desafio brasileiro consiste em conciliar regulação, ética e inovação tecnológica, criando um ambiente institucional que assegure transparência, segurança e confiabilidade dos sistemas automatizados.

O Brasil, embora disponha de bases importantes como o Marco Civil da Internet e a LGPD, ainda carece de um marco jurídico específico para IA e conteúdos sintéticos, o que reforça a urgência de políticas públicas e legislação especializada que assegurem a compatibilização entre inovação tecnológica e proteção dos direitos da personalidade.

## 3 DA ATUAL INSUFICIÊNCIA DE NORMAS E SANÇÕES PARA EM RELAÇÃO AS *DEEPFAKES* NO BRASIL

Como já exposto anteriormente, atualmente o Poder Público ainda carece de normas especificas frente ao combate de *deepfake*, seja normas voltadas para a produção e compartilhamento.

Sob a ótica jurídica, essa problemática se aproxima da noção clássica de responsabilidade por omissão dos provedores e desenvolvedores.

Nigri (2001) já destacava que o provedor que, notificado oficialmente, não retira do ar conteúdo ilícito pode ser considerado coautor do crime. Por analogia, entende-se que os desenvolvedores e mantenedores de sistemas de IA também devem responder solidariamente quando não adotam mecanismos de prevenção e

detecção de usos indevidos, especialmente em casos de reprodução sintética de imagens e vozes sem consentimento.

Por falta de norma especifica, José Estevam Macedo Lima (2022), já observou que:

> por trás da inteligência artificial há necessariamente um humano responsável pela criação do banco de dados ou pela inserção das informações. A IA, portanto, não pode ser tratada como sujeito autônomo moralmente responsável, pois sua atuação decorre de decisões humanas preexistentes. Há, portanto, uma cadeia de responsabilidade que deve abranger desde o programador até o usuário final, Lima (2022).

Apesar da existência de políticas internas em algumas plataformas de IA, como filtros de detecção de conteúdos sensíveis ou mecanismos de denúncia, elas se mostram superficiais, ineficazes e facilmente contornáveis.

As próprias empresas criadoras reconhecem que esses sistemas não impedem a manipulação fraudulenta. Conforme catálogo do site especializado em publicar e disponibilizar diferente tipos de Inteligência Artificial, existem mais de 500 inteligências artificiais generativas gratuitas em operação global (AIXPLORIA, 2025)

Não obstante, existem cerca de 15.000 mil IAs ativas apenas nos Estados Unidos (Forbes, 2025). Tal número significativo demonstra que a política interna superficial para inibir o usuário de praticar condutas ilícitas não passa de um protocolo usual que não gerará resultados frutíferos para a sociedade.

Dado os rumos que a sociedade está caminhando junto as *deepfakes*, depender de apenas política internas de Inteligência Artificial é o mesmo que empurrar o problema para gerações futuras, negligenciando os danos e prejuízos causados todos os dias.

Essa constatação leva à conclusão de que as políticas internas das IAs não bastam, elas não possuem força normativa, sanção coercitiva, nem mecanismos de fiscalização externos.

Além disso, há um evidente conflito de interesses, já que o mesmo agente econômico que cria e lucra com o uso dessas ferramentas seria responsável por restringi-las. Essa autolimitação é, portanto, ilusória e insuficiente.

Diante disso, a alternativa mais viável consiste em estabelecer normas jurídicas complementares às políticas internas, capazes de garantir responsabilização em cadeia, transparência algorítmica e governança compartilhada entre Estado, iniciativa privada e sociedade civil.

Tal estrutura se aproxima dos modelos previstos no Regulamento (UE) 2024/1689, *AI Act*, que define obrigações graduais conforme o grau de risco do sistema e impõe deveres de rastreabilidade, auditoria e identificação explícita de conteúdos manipulados.

Portanto, delegar à própria Inteligência Artificial o papel de regular sua conduta é um equívoco conceitual e ético. A máquina não possui consciência moral, senso de responsabilidade ou discernimento sobre o impacto de suas ações. O

verdadeiro controle deve permanecer nas mãos do ser humano seja o desenvolvedor, o usuário ou o Estado.

Nessa relação tipificar o agente e restringir as IAs, se alinha à crítica feita por Graça (2018) ao observar que o legislador brasileiro, em vez de buscar soluções estruturais e de longo prazo, tende a reagir com imediatismo e vieses punitivistas diante de fenômenos sociais e tecnológicos complexos. Conforme o autor:

> Percebe-se um senso de imediatismo do legislador brasileiro, que possivelmente se vê atacado e defenestrado nas redes sociais e na internet em razão da descrença da sociedade brasileira com os projetos políticos e a falta de legitimidade social. No parlamento brasileiro, as tentativas de regulamentação perpassam, na maioria das vezes, pela criação de um tipo penal que, necessariamente, criminalize as condutas praticadas. O legislador brasileiro parte do pressuposto de que a criação de tipos penais para os indivíduos que pratiquem os verbos nucleares da conduta (divulgar, compartilhar, modificar e desvirtuar a verdade) seria a panaceia para resolver um tema complexo, poroso, o qual exige um estudo aprofundado (GRAÇA, 2019, p. 15)

A reflexão de Graça demonstra que o foco excessivo em punições penais desvia a atenção da real necessidade de uma política regulatória abrangente e técnica, voltada à prevenção, à transparência e à responsabilidade compartilhada.

Assim, o enfrentamento das *deepfakes* deve ir além da criminalização: é preciso instituir um marco jurídico sólido, que trate o tema sob a ótica da ética digital e da proteção social.

A ausência de uma política pública abrangente nesse sentido deixa o Brasil vulnerável, com uma legislação fragmentada e anacrônica.

Em síntese, o cenário brasileiro exige um marco legal específico para a Inteligência Artificial e seus conteúdos derivados, que trate não apenas de punições, mas de prevenção, regulação técnica e responsabilidade compartilhada.

A experiência internacional mostra que a regulação da IA não deve significar censura, mas instrumento de transparência e justiça digital, capaz de proteger a sociedade sem sufocar a inovação.

## 3.2 O Projeto de Lei nº 2.338/2023 como Marco Regulatório para a Inteligência Artificial no Brasil

Diante do cenário de evidente insuficiência normativa e da ausência de instrumentos eficazes para coibir os danos causados pelas *deepfakes*, o Projeto de Lei nº 2.338/2023 surge como uma resposta promissora e necessária.

A proposta busca estabelecer um marco regulatório específico para a inteligência artificial no Brasil, aproximando-se dos parâmetros internacionais e trazendo uma estrutura principiológica sólida para equilibrar inovação, ética e responsabilidade.

Souza e Roveroni (2023) entendem que a regulamentação não deve sufocar a criatividade e o progresso tecnológico, mas sim definir as regras do jogo para

garantir que a inovação ocorra dentro de limites éticos e legais. Isso é particularmente relevante em áreas como a saúde, onde a IA pode ser utilizada em diagnósticos e tratamentos médicos.

Regulamentações sólidas são essenciais para assegurar a segurança dos pacientes e a eficácia dos tratamentos e limitações jurídicas baseados em criação artificial.

Os autores também pontuam que a regulamentação da IA não é apenas uma questão de proteção dos direitos individuais, mas também de preservação dos princípios democráticos. À medida que as IAs passam a desempenhar papéis significativos na tomada de decisões políticas, é fundamental que essas decisões sejam transparentes e justificáveis.

Já Pereira (2024) destaca que, no âmbito do Direito Civil, a personalidade jurídica refere-se à concessão de direitos e obrigações reconhecidos a pessoas físicas ou jurídicas. No contexto da atribuição de autonomia legal às máquinas utilizadas pela inteligência artificial, é essencial considerar as responsabilidades dos usuários e, principalmente, dos desenvolvedores desses dispositivos tecnológicos.

Novo (2022) menciona que, para atribuir limites, seria necessária uma legislação que obedecesse aos princípios inerentes à Constituição Federal, além de abranger a extensa gama de assuntos passíveis de regulamentação.

Não obstante, neste ponto crítico em que a sociedade brasileira, juntamente com os entes federativos, sofre diretamente os impactos provocados pelas *deepfakes*, deve-se analisar a possibilidade de criar não apenas políticas voltadas à imposição de limites, mas também mecanismos de ordem e responsabilidade aplicáveis especificamente à inteligência artificial.

Não há dúvida de que a Inteligência Artificial constitui um tema central para o desenvolvimento social e econômico do país, e deixá-la à deriva, sem direção normativa, equivale a comprometer o próprio avanço nacional.

Nesse sentido, o Projeto de Lei nº 2.338/2023, em tramitação no Congresso Nacional, apresenta uma proposta sólida e abrangente para a criação do marco legal da inteligência artificial no Brasil, buscando equilibrar o desenvolvimento tecnológico com a proteção dos direitos fundamentais e o fortalecimento da governança digital.

A estrutura normativa proposta inspira-se em modelos internacionais, especialmente no Regulamento Europeu de Inteligência Artificial (*AI Act*), mas adapta seus preceitos à realidade jurídica brasileira.

Logo em seus dispositivos iniciais, o PL estabelece que a regulação da inteligência artificial deve ter como eixo central o respeito à dignidade da pessoa humana, à democracia e aos direitos fundamentais, reforçando o caráter ético e protetivo da norma.

Nos artigos 17 a 24, o legislador trata das hipóteses de governança e transparência, impondo aos desenvolvedores, fornecedores e operadores de sistemas de IA a adoção de práticas de segurança, mitigação de riscos e supervisão humana efetiva.

> Art. 17. Os agentes de IA deverão garantir a segurança dos sistemas e o atendimento dos direitos de pessoas ou grupos afetados, nos termos de regulamento.

Também trata medidas especificas tanto para o aplicador quanto para o desenvolvedor previstas nos incisos do Art. 18 do PL 2338/234. Esses dispositivos determinam a responsabilização jurídica de imagens, áudios e vídeos gerados artificialmente sejam identificados e rotulados de forma explícita, de modo a prevenir a disseminação de *deepfakes* e outras manipulações digitais e responsabilizando o verdadeiro culpado, seja o provedor ou agente.

O texto também impõe ao poder público o dever de adotar protocolos de transparência e prestação de contas, assegurando que a utilização de sistemas automatizados por órgãos estatais seja sempre acompanhada de mecanismos de revisão e justificativa das decisões.

No Capítulo V abrange os artigos 35 a 39 visando a responsabilidade civil dos agentes de inteligência artificial. O texto estabelece a aplicação do Código de Defesa do Consumidor em situações de dano decorrente de sistemas utilizados em relações de consumo, adotando, portanto, o regime de responsabilidade objetiva, em que o dever de indenizar independe da comprovação de culpa.

Além disso, o PL amplia a responsabilização para todas as relações jurídicas, determinando que os agentes de IA desenvolvedores, distribuidores e usuários respondem também conforme o Código Civil e outras normas específicas.

Ou seja, em outras palavras, essa PL que traz o Marco da Inteligência Artificial ao sistema jurídico do Brasil preenche as lacunas em que hoje o estado sofre preenchendo supletivamente.

Um dos avanços mais relevantes é a previsão de inversão do ônus da prova (art. 37) nos casos em que a vítima for hipossuficiente ou tecnicamente incapaz de demonstrar o nexo de causalidade entre o dano sofrido e o funcionamento da IA.

> Art. 37. O juiz inverterá o ônus da prova quando a vítima for hipossuficiente ou quando as características de funcionamento do sistema de IA tornarem excessivamente oneroso para a vítima provar os requisitos da responsabilidade civil.

Essa inovação processual fortalece a proteção dos cidadãos diante de sistemas de alta complexidade, reconhecendo a assimetria de informação entre usuários e provedores tecnológicos.

Além disso, o PL prevê que, em ambientes experimentais (*sandbox regulatórios*), os agentes deverão cumprir deveres mínimos de segurança e transparência, mesmo durante as fases de teste e inovação, mantendo a responsabilidade por danos eventualmente causados.

Os artigos 40 e 41, que compõem o Capítulo VI, abordam a autorregulação e os códigos de boas práticas, incentivando as empresas e instituições a criarem programas internos de governança, com auditorias periódicas, canais de denúncia e políticas de ética tecnológica.

O projeto estimula a cooperação entre os setores público e privado, promovendo o desenvolvimento de padrões de compliance algorítmico e diretrizes de conduta que assegurem a transparência e a equidade no uso das inteligências artificiais.

O artigo 42, por sua vez, dispõe sobre a comunicação obrigatória de incidentes graves, determinando que os agentes responsáveis pelos sistemas de IA comuniquem às autoridades competentes qualquer falha ou evento que possa afetar direitos fundamentais, a liberdade de expressão ou o processo democrático.

Essa previsão aproxima-se do regime de notificação de incidentes previsto na Lei Geral de Proteção de Dados (LGPD), consolidando um ecossistema jurídico pautado na prevenção e na mitigação de danos.

Nos dispositivos finais, o projeto dedica especial atenção ao tema da fiscalização e sanções, previstas nos artigos 50 a 52, prevendo multas de até R$ 50.000.000,00 (cinquenta milhões de reais).

A gradação das sanções observa o princípio da proporcionalidade, sendo aplicadas conforme o risco e a gravidade da infração. A fiscalização será exercida por meio do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA), que coordenará as ações entre as agências reguladoras e demais órgãos públicos.

Com essa estrutura, o Marco da Inteligência Artificial propõe um modelo normativo preventivo, técnico e ético, rompendo com o imediatismo punitivista que historicamente marca a legislação brasileira em temas tecnológicos.

Ao reconhecer a importância da responsabilidade compartilhada entre desenvolvedores, operadores e usuários, o projeto distingue, de forma categórica a responsabilidade e sanção de cada indivíduo que contribuiu com o uso mal intencionado da Inteligência Artificial.

Em outras palavras, o Estado passa a ter condições de enfrentar de maneira mais eficaz a disseminação das *deepfakes*, reduzindo os prejuízos sociais e jurídicos gerados pela carência de normas regulatórias próprias.

Assim, o PL 2.338/2023 representa mais do que uma resposta legislativa à expansão das inteligências artificiais: ele simboliza um novo paradigma de regulação digital.

Tabela 1 – Comparativo entre o AI Act (Regulamento UE 2024/1689) e o PL 2.338/2023 (Marco Legal da IA – Brasil)

| **Eixo de Comparação** | **AI Act – União Europeia (Regulamento 2024/1689)** | **PL 2.338/2023 – Brasil (Marco da IA)** |
|---|---|---|
| **Abordagem regulatória** | Estabelece uma estrutura obrigatória e abrangente para sistemas de IA em toda a União Europeia, com abordagem baseada em risco dividida em quatro níveis (proibido, alto, limitado e mínimo). Visa garantir segurança, transparência e conformidade técnica. | Define princípios e diretrizes gerais de governança ética da IA, possui detalhamento baseada em risco (excessivo, alto) sobre e categorização de grau de risco da IA. Também visa garantir segurança, transparência e conformidade técnica. |

| | | |
|---|---|---|
| **Governança, fiscalização e sanções** | Cria autoridades nacionais e o *European Artificial Intelligence Board*, com poder de fiscalização e imposição de sanções severas. As multas podem chegar a 35 milhões de euros ou 7% do faturamento global da empresa. | Prevê a criação do Sistema de Regulação e Governança de IA (SIA) no qual consta possíveis multas de 50 milhões de reais e procedimentos sancionais. |

*Fonte:* Elaborado pelo autor (2025), com base entre o AI Act (2024) e o PL 2.338/23 (2023).

Laura Schertel (2025), relatora da Comissão de Juristas, complementa que não regular seria deixar o cidadão brasileiro à mercê de sistemas que podem ser discriminatórios; que muitas vezes decidem o futuro com base no passado, sem a possibilidade de correção ou supervisão; seria deixar as empresas brasileiras à mercê de uma enorme insegurança jurídica.

Inclusive, nesse mesmo segmento, é imperativo destacar que devem ser observados, em todos os sentidos, os limites entre censura e regulação parcial, voltados à prevenção de qualquer vantagem política ou social.

Conforme apontam Gabriel, Peschl e Whittlestone (2021), a justiça aplicada à inteligência artificial não deve ser compreendida apenas como um valor ético abstrato, mas como um princípio estrutural que orienta o desenvolvimento e o uso dessas tecnologias.

Hoje o Brasil, assim como o restante do mundo, sofre com os impactos causados pelas *deepfakes*. Deixar a sociedade e o poder público reféns dessa tecnologia representa, em uma análise minimalista, um ato de negligência deliberada.

Como já exposto neste estudo, existem medidas legislativas já sancionadas e projetos de lei em tramitação no Congresso, além de experiências internacionais que produzem resultados concretos.

Deixar o fenômeno da inteligência artificial à ausência de controle seria praticamente contribuir, de forma indireta, para o próprio caos digital. A liberdade absoluta de apenas um dos lados da moeda não representa liberdade, mas sim a ausência de equilíbrio e responsabilidade.

Para Bauer (2021), a liberdade, quando interpretada de forma justa, é o que sustenta uma democracia constitucional. Sem dúvida, nesse momento crítico da sociedade, é de senso comum a vulnerabilidade frente às *deepfakes*.

Impor liberdade irrestrita, protegendo apenas um lado e desamparando o outro, sem medidas de segurança, gera mais insegurança jurídica e sensação de vulnerabilidade social.

Hobbes, em sua obra *Leviatã* (1651), mesmo sem imaginar fenômenos tecnológicos como as *deepfakes*, já destacava que os seres humanos, em estado de natureza, estão sempre supondo o que o outro pode estar planejando contra seu semelhante.

Apesar do confronto entre iguais, nenhum indivíduo é capaz de conhecer plenamente as intenções do outro, o que naturalmente gera insegurança e receio diante da possibilidade de ataque.

Nesse sentido, na sociedade contemporânea, há sujeitos que, por partilharem a mesma condição de igualdade e racionalidade, não deveriam ser objeto de limitação ou controle excessivo por parte do Estado Democrático, respeitando em todos os termos a Constituição Federal.

Entretanto, aquele que utiliza a Inteligência Artificial como instrumento de manipulação não se encontra em um contexto de equilíbrio social e jurídico, visto que está munido de uma arma contemporânea irrestrita.

Os autores defendem que a liberdade de criação e inovação técnica deve estar subordinada a padrões de justiça distributiva e proteção da dignidade humana, sob pena de reproduzir e ampliar desigualdades já existentes na sociedade.

Nesse mesmo sentido, Barroso (2009) já advertia que a proteção dos direitos fundamentais não pode se transformar em instrumento de censura, sob pena de comprometer a própria democracia.

De acordo com Salgado, interpretando Kant, afirma que a justiça não deve ser entendida de forma linear, mas flexível, adaptando-se às finalidades sociais (CARVALHO E SOUZA, 2024, P. 79).

A ausência de limites não é sinônimo de liberdade; ao contrário, conduz ao caos, à imprevisibilidade e à impunidade. Nesse ambiente digital desregulado, indivíduos e sistemas agem de forma autônoma e sem controle, criando uma "guerra fria" contemporânea de informações falsas e manipuladas.

Quando o poder público estabelece parâmetros para o uso da inteligência artificial, não sufoca a criatividade: delimita um espaço seguro para que ela floresça. A liberdade criativa só é plena quando exercida em um ambiente ético, previsível e justo.

Se, por um lado, a ausência de regulação conduz ao caos e à desordem, por outro, o excesso de controle pode sufocar a liberdade e comprometer os valores democráticos. A linha que separa proteção de censura é tênue e exige do Estado uma postura equilibrada e proporcional.

A censura nasce quando o poder de regular ultrapassa o limite da razão e impõe restrições arbitrárias ao pensamento e à expressão. Nesse ponto, a regulação deixa de ser uma garantia de liberdade e se transforma em seu oposto: um instrumento de dominação.

Em suma, a regulação eficaz é aquela que protege sem sufocar. Trata-se de um exercício de equilíbrio entre poder e liberdade uma linha tênue que, se ultrapassada, transforma a justiça em autoritarismo e a proteção em opressão, mas, se ignorada, pode gerar uma verdadeira anarquia digital.

Nesse sentido, a tese regulatória através do PL 2338/23, é um refúgio estrutural, onde, inspirado em resultados concretos pelos marcos regulatórios da União Europeia, trará uma sensação de justiça por parte da sociedade brasileira.

## CONSIDERAÇÕES FINAIS

O fenômeno das *deepfakes* expôs um descompasso crítico entre a velocidade do avanço tecnológico e a capacidade de resposta do ordenamento jurídico brasileiro.

Não se trata apenas de falsificação/manipulação sofisticada, mas de um instrumento que cumpre fielmente sua finalidade de manipular, seja qual for o material e o contexto, produzindo impactos direto sobre a honra, a imagem, a privacidade e a própria confiança jurídica social.

Ao longo do estudo, demonstrou-se que a liberdade tecnológica absoluta e a censura são polos inversamente proporcionais. A ausência de limites e imposição do Estado abre caminho para danos significativos e, muitas vezes, irreversíveis.

A restrição excessiva, por sua vez, ameaça silenciar o dissenso e adoece o debate democrático. O desafio é construir uma via regulatória proporcional e transparente.

Do ponto de vista normativo, há avanços, embora que tímidos, o estado já se posicionou quanto a necessidade de dizer basta as *deepfakes*, porém, até o momento, sem grandes movimentos. Por mais que exista a tramitação da PL 2338/23, até o momento, o poder judiciário tem que se ancorar em legislação suplente.

Diante todo o exposto, é necessário um marco legal específico para conteúdos sintéticos, com foco em risco, salvaguardas técnicas, devida diligência de provedores e mecanismos céleres de resposta a incidentes, sem abdicar de garantias processuais. Uma medida eficaz deve operar em camadas transparentes.

Ao adaptar essas referências, o Brasil deixará as leis usadas analogicamente para ser utilizada exclusivamente para a finalidade que foram criadas, e não para tapar buracos de um problema catastrófico.

Em síntese, as *deepfakes* colocam um desafio que é, ao mesmo tempo, tecnológico, jurídico e humanitário, proteger a verdade pública e os direitos da personalidade sem abdicar da liberdade que sustenta a democracia. O equilíbrio é exigente, difícil, mas possível.

## REFERÊNCIAS


AFFONSO, Filipe José Medon. O direito à imagem na era das deepfakes. Revista Brasileira de Direito Civil, v. 27, n. 1, p. 251-251, 2021.

AGÊNCIA BRASIL. Apenas 37% de quem usa internet somente no celular checam informações. 2023. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2023-05/apenas-37-de-quem-usa-internet-somente-no-celular-checam-informacoes Acesso em 23 out 2025.

AIxploria. All Free AI Tools – Page 161. [S.l.], 2025. Disponível em: https://www.aixploria.com/en/free-ai/page/161/?filter=gratuit

BARROSO, Luís Roberto. O Novo Direito Constitucional Brasileiro: Contribuições para a construção teórica e prática da jurisdição constitucional no Brasil. 6. ed. São Paulo: Saraiva, 2012.

BELEZA, Gabriel Pinheiro. A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18? Monografia (Bacharelado em Direito) — Faculdade de Direito, Universidade de Brasília, Brasília, DF, 17 maio 2021. Disponível em: https://bdm.unb.br/bitstream/10483/29391/1/2021_GabrielPinheiroBeleza_tcc.pdf Acesso em 23 de out de 2025.

BITTAR, Carlos Alberto. Os Direitos da Personalidade. 7ed. Rio de Janeiro: Forense Universitária. 2004

BOLESINA, Iuri; GERVASONI, Tássia Aparecida. A proteção do direito fundamental à privacidade na era digital e a responsabilidade civil por violação do direito à extimidade. Novos Estudos Jurídicos – Eletrônica, Itajaí (SC), v. 27, n. 1, p. 87-109, 2022. DOI: 10.14210/nej.v27n1.p87-109. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/16093

BOLSONI, R. A inteligência artificial e o impacto no direito brasileiro. Revista de Negócios e Direito – UNIVALI, 2020. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/16093/10742 Acesso em 24 de out de 2025.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União: Seção 1, Brasília, DF, p. 1, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 21 out 2025.

BRASIL. Lei nº 15.123, de 25 de abril de 2025. Agrava pena para crime de violência contra a mulher com uso de inteligência artificial. Disponível em: https://www12.senado.leg.br/noticias/materias/2025/03/19/pena-maior-para-crime-com-uso-de-ia-contra-a-mulher-vai-a-sancao Acesso em 21 out de 2025.

BRASIL. Presidência da República. Leis sancionadas por Lula avançam na proteção das mulheres contra agressões físicas, psicológicas e digitais. Disponível em: https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2025/04/leis-sancionadas-por-lula-avancam-na-protecao-das-mulheres-contra-agressoes-fisicas-psicologicas-e-digitais Acesso em 22 out de 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 794.586/RJ. Relator: Ministro Raul Araújo. Quarta Turma. Data de Julgamento: 15 mar. 2012. DJe 21 mar. 2012.

BRASIL. Projeto de Lei n.º 2.338, de 2023: “Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana.” Internet: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023 Acesso em 28 out 2025.

CABARAL, Robert Lessa. Deepfake: el futuro de la manipulación audiovisual. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7525024 Acesso em 23 de out de 2025.

CAMARGO, Cláudio. Dignidade da Pessoa Humana na Constituição Federal de 1988. Disponível em: https://www.jusbrasil.com.br/artigos/dignidade-da-pessoa-humana-na-constituicao-federal-de-1988/315805239 Acesso em 23 e out de 2025.

CARTA CAPITAL. Candidata à reeleição em Bauru (SP) é vítima de deepfake em campanha. 2024. Disponível em: https://www.cartacapital.com.br/politica/candidata-a-reeleicao-em-bauru-sp-e-vitima-de-deepfake-em-campanha/ Acesso em 24 de out de 2025.

CEDILLO LAZCANO, Israel. Book Review: *Innovation and the State. Finance, Regulation, and Justice*, by Cristie Ford. *SCRIPTed: A Journal of Law, Technology & Society*, v. 16, n. 1, p. 86-94, 2019. DOI: 10.2966/scrip.160119.86. Disponível em: https://script-ed.org/article/book-review-innovation-and-the-state/ Acesso em 28 de out de 2025.

CETIC.br | NIC.br. Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil – CGI.br, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf Acesso em 25 de out de 2025.

CETIC.BR. Privacidade e proteção de dados pessoais: pesquisa 2021. São Paulo: NIC.br, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf Acesso em 24 de out de 2025.

DE SOUZA, Gustavo Cruz; ROVERONI, Antonio José. Inteligência Artificial (IA): O papel crucial da regulamentação. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 10, p. 1982-1993, 2023.

FERRARI, D.; SENNA, F. Convenção de Budapeste e crimes cibernéticos no Brasil. Migalhas, 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil acesos em 24 de out de 2025.

FILAGRANA, Tatiana Conceição dos Reis. Fake News e Eleições: da Liberdade de Expressão à Violação do Direito de Imagem no Estado Democrático de Direito. Dissertação (Mestrado em Direito) – Centro Universitário Internacional – UNINTER, Curitiba, 2021.

FILGUEIRAS, F. Artificial intelligence policy regimes: comparing politics and policy to national strategies for artificial intelligence. Global Perspectives, v. 3, n. 1, p. 32362, Feb. 2022.

FONSECA, E.; SESTI, V.; ANTONITSCH, A.; VANIN, A.; VIEIRA, R. *CORP: Uma abordagem baseada em regras e conhecimento semântico para a resolução de correferências.* Linguamática, v. 9, n. 1, p. 3-18, jul. 2017. DOI: 10.21814/lm.9.1.241. Disponível em: https://www.linguamatica.com/index.php/linguamatica/article/view/459/528 Acesso em 28 de out de 2025.

FORD, Cristie. Innovation and the state: finance, regulation, and justice. New York: Cambridge University Press, 2017.

GRAÇA, Guilherme Mello. Desvelando o Grande Irmão. Fake News e Democracia: novos desafios do direito constitucional contemporâneo. Revista Eletrônica da Faculdade de Direito de Pelotas, v. 5, n. 1.

G1. Como inteligência artificial criou nudes falsos de mais de 100 mil mulheres compartilhados em redes. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/10/21/como-inteligencia-artificial-criou-nudes-falsos-de-mais-de-100-mil-mulheres-compartilhados-em-redes.ghtml Acesso em 24 de out de 2025.

GABRIEL, Iason; PESCHL, Markus; WHITTLESTONE, Jess. Towards a Theory of Justice for Artificial Intelligence. arXiv preprint arXiv:2110.14419v3, 2021. Disponível em: https://arxiv.org/abs/2110.14419

HEINEN, Juliano. Regulação experimental ou sandbox regulatório – compreensões e desafios. Revista da Faculdade de Direito UFPR, Curitiba, v. 68, n. 1, p. 113-136, jan./abr. 2023. ISSN 2236-7284. Disponível em: https://revistas.ufpr.br/direito/article/view/85389. Acesso em: 30 abr. 2023. DOI: http://dx.doi.org/10.5380/rfdufpr.v68i1.85389.

HOBBES, Thomas. Leviatã. Tradução de Rosina D'Angina. São Paulo: WMF Martins Fontes, 2014.

JARDIM, Gustavo Tanger. Fake news, deepfake e outras ameaças virtuais: os desafios da responsabilidade civil na rede mundial de computadores. Revista de Direito da ADVOCEF, v. 20, n. 36, p. 15-28, 2024.

KUBOTA, Luis Claudio; ROSA, Maurício Benedeti. Inteligência artificial no Brasil: adoção, produção científica e regulamentação. In: KUBOTA, Luis Claudio (Org.). Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil. Rio de Janeiro: Ipea, 2024. p. 9-32. Disponível em: https://repositorio.ipea.gov.br/handle/11058/13128.

LALLA, Vejay; MITRANI, Adine; HARNED, Zach. Artificial intelligence: deepfakes in the entertainment industry. WIPO Magazine, Geneva, n. 2, June 2022. Disponível em: https://www.wipo.int/pt/web/wipo-magazine/articles/artificial-intelligence-deepfakes-in-the-entertainment-industry-42620. Acesso em 23 out. 2025.

LOPES JR., Aury. Introdução Crítica ao Processo Penal, Rio de Janeiro: Lumen Juris Editora, 2010, p. 17.

MARAS, Marie-Helen; ALEXANDROU, Alex. Determinando a autenticidade de evidências em vídeo na era da inteligência artificial e na esteira dos vídeos deepfake. The International Journal of Evidence & Proof, v. 23, n. 3, p. 255-262, 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/1365712718807226. Acesso 23 out. 2025.

MIGALHAS. Deep fake news e sua influência no universo feminino. Disponível em: https://www.migalhas.com.br/depeso/282987/deep-fake-news-e-sua-influencia-no-universo-feminino Acesso em 24 de out de 2025.

MINISTÉRIO PÚBLICO DO ESTADO DO MATO GROSSO. Fraudes com deepfake crescem 822% no Brasil, revela pesquisa. Disponível em: https://www.mpmt.mp.br/conteudo/1217/163277/fraudes-com-deepfake-crescem-822-no-brasil-revela-pesquisa Acesso em 21 de out de 2025.

MONTEIRO, Luiz. Direito Digital. Saraiva, 2018.

MURATA, Ana Maria Lumi Kamimura; RITZMANN TORRES, Paula. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? Boletim IBCCRIM, São Paulo, v. 31, n. 368, p. 13-16, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575

NIC.BR – Núcleo de Informação e Coordenação do Ponto BR. Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo Eletrônico 2021. São Paulo: CGI.br, 2022.

NIGRI, Deborah Fisch. Doutrina Jurídica brasileira: Crimes e Segurança na Internet. Caxias do Sul: Plenum, 2001.

NOVO, Arthur Bayler. A inteligência artificial no âmbito jurídico sob a ótica do direito disruptivo: os impactos da ausência de regulamentação no Brasil. 2022.

NUNES, Lorena de Almeida; ANGELINI Neta, Ainah Hohenfeld. Marco regulatório da inteligência artificial: análise do AI Act da União Europeia no tocante à privacidade. Direito UNIFACS – Debate Virtual, v. ?, n. 293, 2024. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/9279

OCDE (2023), "Sandboxes regulatórios em inteligência artificial", OECD Digital Economy Papers, n.º 356, OECD Publishing, Paris, https://doi.org/10.1787/8f80a0e6-en.

PARLAMENTO EUROPEU. Relatório A8-0005/2017 que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica. 27 jan. 2017. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html#_section2

PEREIRA, Amanda Kelly Araújo; MEDEIROS, Denise Rodrigues; PELISSON, Gustavo Chalegre. REGULAMENTAÇÃO DOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO ORDENAMENTO JURÍDICO BRASILEIRO. Revista Multidisciplinar do Nordeste Mineiro, v. 4, n. 1, 2024.

RADU, R. Steering the governance of artificial intelligence: national strategies in perspective. Policy and Society, v. 40, n. 2, p. 178-193, 3 Apr. 2021.

ROBLES-LESSA, Moyana Mariano; CABRAL, Hildeliza Lacerda Tinoco Boechat; SILVESTRE, Gilberto Fachetti. Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. Revista Dialnet, [S.l.], publicação em linha em 1º jul. 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7525024

SENNA, Felipe; FERRARI, Daniella. Convenção de Budapeste e crimes cibernéticos no Brasil. Migalhas – De Peso, 21 out. 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil

SILVA, Cícero Henrique Luís Arantes da. A mídia e sua influência no sistema penal. 2006. Disponível em: https://jus.com.br/artigos/2814/a-midia-e-sua-influencia-no-sistema-penal Acesso em 23 de out de 2025.

STEWART, Fenner. Book Review of *Innovation and the State: Finance, Regulation, and Justice* by Cristie Ford. *Modern Law Review*, v. 82, n. 1, p. 190-194, 2019. Disponível em: https://ssrn.com/abstract=3661732 Acesso em 28 de out de 2025.

SIQUEIRA, Paulo Alexandre Rodrigues de. O ‘Deep Fake’ e a Legislação Brasileira – utilização de instrumentos legais para a proteção à imagem. JusBrasil, 2019. Disponível em: https://www.jusbrasil.com.br/artigos/o-deep-fake-e-a-legislacao-brasileira-utilizacao-de-instrumentos-legais-para-a-protecao-a-imagem/735209926 Acesso em 24 de out de 2025.

SPENCER, Robert. Deep Fake: a última distopia. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/ Acesso 23 out. 2025.

SUPREMO TRIBUNAL FEDERAL. Supremo lança guia ilustrado contra as deepfakes. Disponível em: https://noticias.stf.jus.br/postsnoticias/supremo-lanca-guia-ilustrado-contra-as-deepfakes/ Acesso em 23 de out de 2025.

TACCA, Adriano; ROCHA, Leonel Severo. Inteligência Artificial: reflexos no sistema do direito. UFC, 2018.

TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO. Direito Hoje | As liberdades políticas na era digital. Uma leitura conforme a teoria rawlsiana / Luciana Dias Bauer, 12 jul. 2021. Disponível em: https://www.trf4.jus.br/trf4/controlador.php?acao=pagina_visualizar&id_pagina=1799

UEVA, Ricardo Villas Bôas. Fake news e liberdade de expressão. JOTA, 2018. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-expressao/fake-news-stj Acesso em 23 de out de 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Diário Oficial da União Europeia, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

WORKMIND. How Many AI Tools Are There? [s.l.], 9 fev. 2025. Disponível em: https://workmind.ai/how-many-ai-tools-are-there/

YOUNG, Norbert. DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media. Edição Kindle. 2019.

ZAFFARONI, Eugenio Raúl. A questão criminal. Rio de Janeiro: Revan, 2013. 320 p. Tradução Sérgio Lamarão.EPUB.