

**DA FRANÇA AO BRASIL: UM ESTUDO DE DIREITO
COMPARADO PARA A REDUÇÃO DE RISCOS
DA DEEPFAKE NO BRASIL**

Universidade Presbiteriana Mackenzie

Coordenadoria de Fomento à Pesquisa - Pró-Reitoria de Pesquisa e
Pós-Graduação

Reinaldo Medeiros Dias Souza Dourado

Apoio: Pivic Mackenzie

Ms. Carlos Luiz de Lima e Naves

Universidade Presbiteriana Mackenzie, Campus Campinas - CCT

Universidade Presbiteriana Mackenzie, Campus Campinas - CCT

10400411@mackenzista.com.br

carlos.naves@mackenzie.br

RESUMO

A presente pesquisa analisa o fenômeno dos deepfakes e sua regulamentação jurídica, estabelecendo um estudo comparativo entre a legislação francesa e brasileira. Com o avanço exponencial das tecnologias de inteligência artificial, especialmente aquelas capazes de gerar conteúdo sintético indistinguível da realidade, emerge uma necessidade premente de marcos regulatórios eficazes. O estudo examina como a França, inserida no contexto normativo da União Europeia, tem enfrentado os desafios jurídicos impostos pelos deepfakes, e como essas experiências podem contribuir para o aperfeiçoamento do ordenamento jurídico brasileiro. A metodologia empregada consistiu em análise documental comparativa, exame de legislações, jurisprudência e doutrina especializada. Os resultados indicam que a abordagem francesa, fundamentada em princípios de responsabilização das plataformas digitais e criminalização específica de condutas, oferece subsídios valiosos para o aprimoramento da legislação brasileira, especialmente considerando as recentes decisões do Supremo Tribunal Federal sobre o Marco Civil da Internet. Conclui-se que a adoção de um modelo híbrido, que incorpore elementos da experiência francesa adaptados à realidade constitucional brasileira, pode representar um caminho promissor para a regulamentação efetiva dos deepfakes no Brasil.

Palavras-chave: Deepfake; Inteligência Artificial; Direito Comparado; Sociedade de Riscos; Regulamentação;.

ABSTRACT

This research analyzes the deepfake phenomenon and its legal regulation, establishing a comparative study between French and Brazilian legislation. With the exponential advancement of artificial intelligence technologies, especially those capable of generating synthetic content indistinguishable from reality, an urgent need for effective regulatory frameworks emerges. The study examines how France, within the European Union regulatory context, has faced the legal challenges posed by deepfakes, and how these experiences can contribute to improving the Brazilian legal system. The methodology employed consisted of comparative documentary analysis, examination of legislation, jurisprudence, and specialized doctrine. The results indicate that the French approach, based on principles of digital platform accountability and specific criminalization of conduct, offers valuable insights for improving Brazilian legislation, especially considering recent Supreme Court decisions on the Internet Civil Framework. It is concluded that adopting a hybrid model, incorporating elements from French experience adapted to Brazilian constitutional reality, may represent a promising path for effective deepfake regulation in Brazil.

Keywords: Deepfake; Artificial Intelligence; Comparative Law; Regulation; Risk Society.

1. INTRODUÇÃO

O século XXI testemunha uma revolução tecnológica sem precedentes,

caracterizada pela democratização de ferramentas de inteligência artificial capazes de manipular a realidade de forma cada vez mais sofisticada. Entre essas tecnologias, os deepfakes emergem como um fenômeno particularmente desafiador para o ordenamento jurídico contemporâneo, suscitando questões fundamentais sobre autenticidade, privacidade, dignidade humana e responsabilidade civil e penal diante dos riscos que a sua má utilização pode representar.

Os deepfakes, termo derivado da combinação das palavras "deep learning" e "fake", representam uma categoria de mídia sintética produzida por algoritmos de aprendizado profundo, capazes de criar vídeos, áudios e imagens que parecem autênticos, mas que na realidade são artificialmente gerados ou manipulados (CITRON; CHESNEY, 2019). Essa tecnologia, inicialmente restrita a laboratórios de pesquisa e grandes corporações, tornou-se progressivamente acessível ao público geral, ampliando exponencialmente seu potencial de uso e, conseqüentemente, de abuso.

A facilidade crescente de criação e disseminação de conteúdo sintético levanta preocupações legítimas sobre seu impacto em diversos aspectos da vida social, política e econômica. Desde a criação de pornografia não consensual até a manipulação de discursos políticos, os deepfakes representam uma ameaça multifacetada que demanda respostas jurídicas adequadas e eficazes.

Desse modo, a França emerge como um *case study* particularmente relevante, não apenas por sua tradição jurídica continental, que guarda semelhanças com o sistema brasileiro, mas também por sua inserção no contexto normativo da União Europeia, que tem se mostrado pioneira na regulamentação de tecnologias emergentes.

A recente entrada em vigor do AI Act europeu, que inclui disposições específicas sobre deepfakes, representa um marco regulatório importante que estabelece obrigações específicas para sistemas geradores de conteúdo sintético. O regulamento europeu institui requisitos de rotulagem obrigatória para conteúdo artificialmente gerado, exigindo que usuários sejam claramente informados sobre a origem sintética do material, além de implementar sistemas de transparência que permitem rastreabilidade do processo de criação.

As plataformas digitais passam a ter responsabilidades ampliadas, incluindo a implementação de sistemas de detecção automatizada, elaboração de relatórios de transparência periódicos e cooperação efetiva com autoridades regulatórias, sob pena de

sanções administrativas que podem alcançar até 6% do faturamento global anual. Esta estrutura regulatória europeia oferece insights valiosos para outros ordenamentos jurídicos, especialmente considerando que o Marco Civil da Internet brasileiro, elaborado em 2014, antecede cronologicamente o desenvolvimento do AI Act, não tendo se inspirado diretamente no projeto europeu, mas criando oportunidades contemporâneas de harmonização normativa que poderiam preencher lacunas identificadas na legislação nacional, particularmente no que se refere à regulamentação proativa de tecnologias emergentes como os deepfakes.

O Brasil, por sua vez, encontra-se em um momento crucial de sua história digital. O país, que já conta com marcos normativos importantes como o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (Lei 13.709/2018), está passando por um processo de revisão e atualização de suas normas para o ambiente digital, especialmente após as recentes decisões do STF sobre a responsabilização de plataformas digitais.

Portanto, tem-se como problema principal, o questionamento de: como a ausência de regulamentação específica sobre deepfakes no Brasil compromete a proteção de direitos fundamentais e a segurança jurídica, e de que forma a legislação estrangeira, especificamente a francesa, pode oferecer soluções adaptáveis ao contexto jurídico-constitucional brasileiro para reduzir os riscos inerentes à essa nova realidade?

A metodologia empregada nesta pesquisa fundamenta-se em abordagem hipotético-dedutivo com revisão bibliográfica para análise do problema regulatório identificado. A técnica principal consiste na análise legislativa e jurisprudencial entre os ordenamentos jurídicos francês e brasileiro, complementada por um estudo sobre materiais o tema, avaliando desde a legislação francesa específica sobre deepfakes, particularmente a Lei SREN de 2024; a regulamentação europeia, especialmente o AI Act e a legislação brasileira aplicável.. Justifica-se tal exame pela necessidade premente de compreender como diferentes sistemas jurídicos têm enfrentado os desafios impostos pelos deepfakes, buscando identificar soluções que possam ser adaptadas e aplicadas ao contexto brasileiro. A análise comparativa permite não apenas identificar lacunas e oportunidades de aprimoramento, mas também contribuir para o debate acadêmico e legislativo sobre a regulamentação de tecnologias.

Resta assim como objetivo a análise sobre como a legislação francesa pode contribuir para o aperfeiçoamento do marco regulatório brasileiro no que se refere aos

deepfakes a fim de eliminar ou reduzir riscos para a coletividade, desenvolvendo um estudo para compreender a regulamentação de deepfakes na França e o cenário atual no Brasil.

2. DESENVOLVIMENTO DO ARGUMENTO

2.1 DA SOCIEDADE DE RISCOS IMENSURÁVEIS

A conceptualização da "sociedade de risco", desenvolvida pelo sociólogo alemão Ulrich Beck, transcende a mera identificação de perigos circunscritos, evoluindo para uma teoria crítica que diagnostica uma fase histórica na qual os próprios processos de modernização geram ameaças sistêmicas, globais e de consequências frequentemente irreversíveis. Beck (2010, p. 25) estabelece uma distinção fundamental ao argumentar que, diferentemente dos riscos aventureiros da era das navegações, os riscos contemporâneos "não são uma invenção moderna... [mas] riscos pessoais, e não situações de ameaça global, como as que surgem para toda a humanidade como a fissão nuclear ou com o acúmulo de lixo nuclear". Esta transição do risco pessoal para a ameaça global constitui o cerne da sociedade de risco, onde a produção social de riqueza torna-se indissociável da produção social de perigos de natureza antropogénica, deslocando os conflitos sociais clássicos da distribuição de bens para a distribuição de males (BECK, 2011, p. 23).

Neste panorama, os deepfakes emergem não como mais uma ferramenta de ilícito, mas como a epitomização do risco tecnológico moderno: produtos de uma inteligência artificial desvinculada de um marco ético-jurídico robusto, capazes de corroer os alicerces epistemológicos da verdade factual e da confiança interpessoal, que são os alicerces do contrato social. A profundidade e imensidão deste risco não residem apenas na capacidade técnica de falsificação hiper-realista, mas na indistinção deliberada entre o real e o sintético, criando uma zona cinzenta de incerteza radical onde a própria percepção da realidade é posta sob suspeita permanente. Esta "crise do real", na qual a tecnologia não ameaça apenas bens jurídicos individuais, mas a própria possibilidade de consenso social, representando um desafio considerável para o Direito (COSTA; NETO, 2024).

A sociedade, assim, não teme apenas um dano concreto e reparável, ela enfrenta a perspectiva da implosão dos mecanismos cognitivos coletivos que permitem aferir a veracidade, a autenticidade e a confiança, fundamentos sem os quais a vida democrática e a própria coexistência pacífica se tornam impossíveis. A deepfake é, portanto, um risco imensurável porque o seu dano potencial é ontológico e civilizacional, e não meramente jurídico-individual. Como salienta Prittwitz (2004, p. 39), o Direito Penal moderno, na sua tentativa de responder a estes riscos de nova natureza, sofre uma mutação profunda em direção a um direito que se expande, caracterizado pela admissão de novos bens jurídicos penalmente relevantes, pelo deslocamento da fronteira entre o punível e o não-punível para fases cada vez mais precoces da conduta (antecipação da tutela penal), e pela "redução das

exigências de censurabilidade", frequentemente em detrimento de garantias e princípios fundamentais consagrados pelo Estado de Direito. A regulação dos deepfakes, neste contexto, não se insere num debate penal comum sobre a tipificação de novas condutas, mas num dilema civilizatório muito mais profundo sobre como preservar a verdade, a dignidade humana e a autonomia individual num ecossistema digital deliberadamente arquitetado para confundir, manipular e polarizar.

A reflexividade, outro pilar central da teoria de Beck, é a chave para compreender a complexidade da resposta exigida. A modernidade reflexiva é aquela que volta seu olhar crítico para si mesma, confrontando-se com as consequências não intencionais e frequentemente catastróficas de seu próprio desenvolvimento tecnológico e científico. A deepfake é o epítome deste processo de autorreflexão forçada: a inteligência artificial, culminação do projeto moderno de domínio racional da natureza através da técnica, volta-se contra a sociedade que a criou, ameaçando corroer a confiança interpessoal e institucional que é a base de todo o tecido social. Como observa Costa (2024, p. 3) em análise pertinente, "a modernidade atual traz constantes mudanças em todas as esferas da vida em sociedade, gerando dúvidas persistentes que influenciam profundamente o campo do direito penal". A regulação da deepfake não pode, portanto, ser uma reação impulsiva, temerosa e guiada pelo pânico moral. Ela deve ser o produto de uma reflexão profunda, informada, multidisciplinar e necessariamente reflexiva, que avalie com rigor não apenas a eficácia potencial da intervenção penal, mas também os seus custos sociais, os seus efeitos colaterais na inovação tecnológica legítima e, sobretudo, o seu impacto nas liberdades fundamentais, em especial a liberdade de expressão e de informação.

A sensação de insegurança gerada por esta nova classe de riscos não é meramente subjetiva ou irracional; é um sintoma estrutural daquilo que Jesús-Maria Silva Sánchez (2013, p. 40) identifica com precisão como a "sociedade da 'insegurança sentida' (ou como a sociedade do medo)", onde a percepção do risco, alimentada pela viralidade midiática e pela velocidade de disseminação da informação, torna-se uma força motriz poderosa para demandas sociais por controlo, vigilância e regulação, nem sempre racionais ou proporcionais. O Direito, e em especial o Direito Penal como *ultima ratio*, é constantemente pressionado a expandir o seu âmbito de atuação para dar uma resposta simbólica a esta angústia social difusa. No contexto brasileiro, esta tensão é palpável e particularmente aguda. De um lado, existe uma demanda social legítima e urgente por proteção contra os usos maliciosos de tecnologias como a deepfake, que representam uma ameaça visceral e imediata à honra, à imagem, à privacidade e à própria integridade dos

processos democráticos. A viralidade de um conteúdo manipulado pode causar danos irreparáveis em questão de horas, tornando as soluções judiciais tradicionais, lentas e meramente reparatórias, manifestamente insuficientes. Por outro lado, essa mesma demanda é frequentemente capturada e amplificada por uma lógica midiática sensacionalista e por ondas de pânico moral, que podem conduzir a reações legislativas precipitadas, desproporcionadas e pouco eficazes. Alves e Kazmierczak (2016, p. 36) alertam precisamente para este perigo, ao constatarem que esta visão distorcida do Direito Penal, "como instrumento de crueldade e de vingança, surge no seio da sociedade que clama por uma punição simbólica para aquele infrator".

O desafio para o legislador e para os aplicadores do direito na sociedade de riscos imensuráveis é, portanto, evitar que a resposta jurídica à deepfake se transforme num instrumento de "crueldade e de vingança" simbólica e ineficaz, que sacrifique garantias e liberdades fundamentais em nome de uma segurança ilusória. Deve-se evitar a tentação de cair na armadilha do chamado "Direito Penal do Inimigo", teoria desenvolvida por Günther Jakobs que, nas palavras dos mesmos autores, retira do inimigo:

"a própria condição de pessoa, pois não é a quantidade de direito de que alguém é privado que lhe anula essa condição, mas sim a própria razão em que essa privação de direitos se baseia, isto é, quando alguém é privado de algum direito apenas porque é considerado puro e simplesmente como um ente perigoso" (ALVES; KAZMIERCZAK, 2016, p. 42, citando ZAFFARONI, 2007, p. 18).

A regulação da deepfake deve, pois, navegar entre o Scila da inação estatal, que deixaria os cidadãos desprotegidos face a uma ameaça nova e devastadora, e o Carídis do pan-penalismo autoritário, que sacrificaria o Estado de Direito em nome de uma segurança totalitária. A lição que fica da teoria da sociedade de risco é que a resposta jurídica aos seus perigos deve ser tão complexa, ponderada, reflexiva e proporcional quanto os próprios riscos que se propõe a enfrentar, sempre tendo a dignidade da pessoa humana como farol intransponível e fundamento de todo o ordenamento jurídico-constitucional. A experiência comparada, notadamente a francesa, mostra que é possível encontrar este equilíbrio delicado através de uma combinação de tipificação penal específica, regulação proativa das plataformas e salvaguardas processuais robustas.

2.2 DIREITOS FUNDAMENTAIS E OS RISCOS DE USUÁRIOS DA INTERNET

O ambiente digital, ao se tornar uma extensão onnipresente e quase indispensável da vida social, econômica, política e afetiva do ser humano do século XXI, transformou-se também no novo palco privilegiado e mais perigoso para a realização e, simultaneamente,

para a violação dos direitos fundamentais. A arquitetura própria da internet, caracterizada pela desterritorialização, pelo anonimato ou pseudonimato, pela velocidade de propagação de informação e pela capacidade de replicação infinita e barata, criou um ecossistema onde os tradicionais conflitos jurídicos assumem uma escala, uma virulência, uma permanência e uma complexidade totalmente inéditas na história.

Neste contexto, a *deepfake* surge não como mais uma ferramenta para a prática de ilícitos já conhecidos, mas como uma verdadeira arma de desestabilização individual e coletiva de precisão e poderio inéditos, capaz de atacar a essência mesma de direitos constitucionalmente consagrados de uma forma que desafia os paradigmas tradicionais de proteção jurídica. A violação perpetrada por uma *deepfake* maliciosa é multifacetada e atinge uma profundidade ontológica raramente vista noutras formas de delito. Em primeiro lugar, ela atinge de forma absolutamente devastadora a honra, a imagem e a privacidade.

Diferentemente de uma injúria, calúnia ou difamação verbal ou escrita, a *deepfake* não alega, ela fabrica uma prova audiovisual falsa, dotada de um poder persuasivo e de uma verossimilhança avassaladores. Ela cria uma narrativa visual e auditiva alternativa que se impõe aos sentidos do espectador com a força do que é "visto e ouvido", causando um dano reputacional de magnitude, profundidade e irreparabilidade absolutamente incomparáveis com as formas tradicionais de ofensa à honra. Uma vez lançada na rede, a imagem falsa torna-se praticamente impossível de ser completamente erradicada, perseguindo a vítima indefinidamente através de *screenshots*, *reup loads* e partilhas em fóruns *closed*, constituindo uma espécie de "dança macabra digital" que se perpetua no tempo.

Em segundo lugar, e de modo ainda mais perverso, a *deepfake* constitui uma violação gravíssima e particularmente traumatizante à intimidade e à vida privada (art. 5º, X, CF/88). A sua utilização para criar pornografia não consensual (*non-consensual deepfake pornography*) representa uma das formas mais cruéis de violência digital, invadindo a esfera mais reservada e íntima da pessoa sem qualquer consentimento e com um realismo aterrador. Este tipo específico de violação, para além do imenso e duradouro sofrimento psíquico que causa, frequentemente visa explicitamente a humilhação, a chantagem (*sextortion*) e a destruição social da vítima, representando uma forma de violência de género e de assédio digital particularmente covarde e devastadora.

Por fim, e de modo mais profundo e filosófico, o uso malicioso de *deepfakes* configura um atentado frontal e direto à dignidade da pessoa humana (art. 1º, III, CF/88), fundamento de todo o Estado Democrático de Direito brasileiro. A dignidade, como bem a

define a doutrina constitucional, é o valor intrínseco, inalienável e indisponível de todo e qualquer ser humano, que impõe o respeito incondicional à sua autonomia, integridade física e moral, e ao seu livre desenvolvimento da personalidade. A deepfake nega radicalmente e de forma existencial esta dignidade ao reduzir o indivíduo a um mero objeto de manipulação digital, um fantoche cuja imagem, voz, gestos e ações podem ser fabricados, distorcidos e instrumentalizados ao bel-prazer de terceiros, sem a sua vontade, contra a sua própria identidade e em negação da sua autonomia moral. Como salienta Greco (2008, p. 24), a dignidade da pessoa humana deve servir de "base para todos os ramos do direito", mas é no Direito Penal, "em virtude das consequências de sua aplicação e severidade de suas armas que atingem sobremaneira o homem e lhe afetam a convivência social e pessoal", que a sua observância se torna mais premente e, paradoxalmente, mais vulnerável em momentos de pânico moral e de demandas sociais por segurança a qualquer custo.

Face a esta nova e aterradora capacidade lesiva, o princípio da intervenção mínima, pedra angular do Direito Penal liberal e garantista, é colocado à prova mais severa e complexa da sua história. Este princípio, que orienta o legislador a tipificar como crime apenas condutas que ofendam bens jurídicos relevantes e que não possam ser eficazmente protegidas e sancionadas por outros ramos do direito (sanções administrativas, indenizações civis), parece, em uma análise superficial e conservadora, contraindicar uma criminalização específica da deepfake. Um argumento de status quo poderia sustentar que o arsenal legal já existente – os crimes contra a honra previstos nos artigos 138 a 140 do Código Penal (calúnia, injúria, difamação), os dispositivos do Marco Civil da Internet (Lei 12.965/2014), a Lei de Crimes Cibernéticos (Lei 12.737/2012) e a ação de reparação por danos morais do Código Civil – seria teórica e formalmente suficiente para coibir a conduta e reparar as vítimas. Contudo, uma análise mais aprofundada e realista revela a insuficiência qualitativa, quantitativa e temporal destes instrumentos face à singularidade desse fenômeno.

A lesividade de uma deepfake não é quantitativamente comparável à de uma notícia falsa escrita ou de um insulto; é uma violação de natureza qualitativamente distinta, que opera em um registro de verossimilhança e persuasão sensorial que corrói a própria capacidade individual e coletiva de discernimento entre o real e o fabricado. O dano que provoca é, como já dito, frequentemente irreparável na prática e de escala viral potencial. Além disso, a autoria é técnica e juridicamente complexa de apurar, e a remoção do conteúdo da internet é uma batalha judicial demorada, custosa e emocionalmente

desgastante contra a *hydra* de múltiplas cabeças das plataformas e dos sites de replicação. Neste cenário, a tipificação penal específica e bem desenhada, desde que pautada pela estrita observância dos princípios da lesividade, da fragmentariedade e da subsidiariedade, pode ser justificada como *ultima ratio* para preencher uma lacuna evidente e intolerável de proteção jurídica efetiva. No entanto, é crucial atentar para o alerta de Wedy (2013, p. 72) sobre os perigos de um sistema penal historicamente seletivo e discriminatório: "não devem ser esquecidas as conquistas no que se refere aos direitos e garantias individuais, assim como uma contenção equilibrada do direito penal, especialmente aos mais suscetíveis de serem 'clientes' de um sistema penal flagrantemente injusto e discriminatório como o brasileiro".

A criminalização, portanto, deve ser cirúrgica, precisa e proporcional, dirigindo-se aos usos efetivamente maliciosos, danosos e socialmente intoleráveis da tecnologia (e.g., para difamar, caluniar, extorquir, assediar, interferir em eleições), e não à tecnologia em si ou a usos lícitos e socialmente valiosos (satíricos, artísticos, educativos, de investigação), sob pena de se criminalizar a inovação, cercear indevidamente a liberdade de expressão e criar um tipo penal vago e inconstitucional.

É justamente no ponto de conflito entre a liberdade de expressão e informação (art. 5º, IX, CF/88) e a proteção de outros direitos fundamentais que a regulação da *deepfake* atinge o seu grau máximo de complexidade e delicadeza constitucional. De um lado, a tecnologia possui aplicações legítimas, socialmente valiosas e merecedoras de ampla proteção no cinema, na publicidade, na arte, na educação e no jornalismo. De outro, o seu uso para fins ilícitos representa um abuso manifestamente censurável dessa liberdade, que deve ser vigorosamente coibido.

O ordenamento jurídico já possui mecanismos tradicionais e principiológicos para resolver este conflito de direitos, baseando-se na ponderação de interesses concretos e no caso específico. A *deepfake*, porém, introduz uma variante perversa e nova neste equilíbrio: a capacidade de fabricar uma "evidência" ou "testemunho" falso de alto poder de convicção e de difícil detecção para o cidadão comum. Isso corrompe e enviesa o próprio processo de ponderação de interesses, pois lança sobre a vítima um ônus probatório esmagador, injusto e praticamente insustentável: o de demonstrar, perante todos e a todo momento, perante plataformas, autoridades e a opinião pública, que um conteúdo audiovisual aparentemente verídico e convincente é, na realidade, uma falsificação tecnológica. Esta inversão prática e de facto do ônus da prova, que transforma a vítima em réu que tem de provar a sua inocência e a falsidade da "prova" apresentada contra si, viola

gravemente a presunção de inocência, o direito ao devido processo legal e o próprio estado de direito material. Neste aspeto, a lição do garantismo penal de Luigi Ferrajoli (2006, p. 91) e o seu axioma "*Nulla accusatio sine probatione*" (não há acusação sem prova) adquirem uma relevância prática e dramática. A *deepfake* é, na sua essência conceptual, uma acusação sem prova legítima; é a prova fraudulenta e má-fé por excelência.

A ausência de uma tipificação penal clara que defina de forma precisa e estrita o ilícito, que estabeleça procedimentos ágeis, extrajudiciais e eficazes para a identificação dos responsáveis e a remoção obrigatória e imediata do conteúdo das plataformas, e que preveja sanções proporcionais e dissuasoras, deixa o utilizador da internet em um estado de vulnerabilidade, desproteção e desamparo jurídico intolerável para uma democracia.

Esta insegurança jurídica generalizada, como bem diagnostica Galdi (2015, p. 45), gera na sociedade a "sensação do descumprimento aparente do direito penal", minando a confiança nas instituições, no sistema de justiça e no próprio Estado, e alimentando um ciclo vicioso de medo, de frustração e de demandas por soluções punitivistas cada vez mais severas e potencialmente autoritárias. Portanto, a regulamentação específica, ponderada, técnica e constitucionalmente orientada da *deepfake* não se configura como uma censura prévia ou uma restrição indevida à liberdade de expressão, mas, paradoxalmente, como uma condição indispensável para a própria efetividade, coexistência pacífica e exercício equilibrado dos direitos fundamentais na esfera digital. Ela é essencial para fornecer segurança jurídica, clareza normativa, previsibilidade e instrumentos processuais eficazes de proteção para todos os atores envolvidos: o Estado, os provedores de aplicação e, acima de tudo, o cidadão, garantindo que a sua dignidade, honra, imagem e privacidade permaneçam invioláveis mesmo face aos mais avançados e aterradores recursos da tecnologia.

2.3 OS DEEPPAKES E A LACUNA REGULATÓRIA BRASILEIRA

A ausência de regulamentação específica sobre deepfakes no Brasil representa um problema jurídico complexo que compromete tanto a proteção de direitos fundamentais quanto a segurança jurídica do ordenamento nacional. Os deepfakes, definidos como conteúdos audiovisuais sintéticos criados através de algoritmos de aprendizado profundo baseados em Redes Adversárias Generativas (GANs), constituem uma tecnologia que permite a criação de material que parecem autênticos mas são inteiramente fabricados (CHESNEY; CITRON, 2019, p. 1757). Esta capacidade técnica de manipulação hiper-realista da imagem e voz humana gera desafios inéditos para sistemas jurídicos que

não foram concebidos para lidar com a falsificação tecnológica de evidências audiovisuais.

O impacto dos deepfakes transcende questões técnicas, adentrando em complexas violações de direitos fundamentais. No âmbito individual, esta tecnologia permite ataques à dignidade humana, honra, imagem e privacidade de forma particularmente perversa, criando conteúdo falso que pode destruir reputações e causar danos psicológicos severos (RÖSSLER, 2021, p. 45-67). No contexto democrático, os deepfakes representam uma ameaça à integridade informacional, permitindo a criação de desinformação sofisticada que pode influenciar processos eleitorais e minar a confiança pública nas instituições (VACCARI; CHADWICK, 2020, p. 2395-2412).

O ordenamento jurídico brasileiro, apesar de possuir marcos normativos avançados como o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (Lei 13.709/2018), apresenta lacunas significativas no tratamento específico dos deepfakes. O Marco Civil, concebido antes da popularização desta tecnologia, estabelece no artigo 19 um sistema de responsabilização de provedores que exige ordem judicial específica para remoção de conteúdo, modelo que se mostra inadequado para a natureza particularmente danosa e urgente dos casos de deepfakes (BRASIL, 2014). A aplicação analógica dos crimes contra a honra previstos nos artigos 138 a 140 do Código Penal, embora ofereça alguma proteção, revela-se insuficiente para capturar as especificidades técnicas e os danos únicos causados pela falsificação digital (BRASIL, 1940).

Esta inadequação normativa cria um cenário de insegurança jurídica que deixa vítimas de deepfakes sem proteção efetiva e dificulta a atuação do sistema de justiça. A tentativa de aplicação dos crimes contra a honra previstos nos artigos 138 a 140 do Código Penal, embora represente esforço interpretativo legítimo dentro dos limites do princípio da legalidade estrita, revela-se insuficiente para capturar as especificidades técnicas e os danos únicos causados pela falsificação digital. É importante esclarecer que tal aplicação não constitui analogia criminalizante proibida pelo ordenamento penal brasileiro, mas sim interpretação extensiva dentro dos tipos penais existentes, respeitando o princípio *nullum crimen sine lege*. Contudo, os tipos tradicionais de calúnia, difamação e injúria foram concebidos para condutas convencionais de ofensa à honra, não contemplando as particularidades técnicas dos *deepfakes*, como a capacidade de criar evidência audiovisual falsa convincente, a facilidade de disseminação em plataformas digitais e os danos à credibilidade e confiança social que transcendem os prejuízos aos direitos da personalidade.

A ausência de definições legais específicas, procedimentos adequados para casos urgentes e critérios claros para responsabilização de plataformas digitais compromete a efetividade da resposta jurídica brasileira aos desafios impostos pelos deepfakes, evidenciando a necessidade de tipificação específica que garanta segurança jurídica tanto para aplicadores do direito quanto para potenciais infratores e vítimas.

Esta inadequação normativa cria um cenário de insegurança jurídica que deixa vítimas de deepfakes sem proteção efetiva e dificulta a atuação do sistema de justiça. A ausência de definições legais específicas, procedimentos adequados para casos urgentes e critérios claros para responsabilização de plataformas digitais compromete a efetividade da resposta jurídica brasileira aos desafios impostos pelos deepfakes. Recentes iniciativas legislativas, como o Projeto de Lei 146/2024 do Senador Chico Rodrigues, que propõe aumentar penas de crimes tradicionais quando praticados com deepfakes, representam avanços sérios, mas insuficientes para criar um *framework* abrangente (BRASIL, 2024a).

Recentes iniciativas legislativas, como o Projeto de Lei 146/2024 do Senador Chico Rodrigues, que propõe aumentar penas de crimes tradicionais quando praticados com deepfakes, representam avanços importantes no reconhecimento legislativo da gravidade específica dos deepfakes e na sinalização política sobre a necessidade de regulação diferenciada para esta tecnologia. O projeto demonstra evolução na compreensão parlamentar sobre os danos potencializados que deepfakes podem causar quando utilizados para práticas criminosas tradicionais, justificando o agravamento das sanções penais. Contudo, tal iniciativa ainda se revela insuficiente para criar um *framework* regulatório abrangente, uma vez que mantém a dependência de tipos penais tradicionais que foram concebidos para realidades pré-digitais e não contemplam as especificidades dos deepfakes.

O referido projeto não estabelece procedimentos específicos para casos urgentes que exigem remoção imediata de conteúdo, não regulamenta as responsabilidades das plataformas digitais na detecção e remoção proativa de deepfakes maliciosos, e carece de definições técnicas precisas sobre o que constitui deepfake para fins de aplicação legal. Além disso, a proposta não aborda questões fundamentais como mecanismos obrigatórios de detecção, cooperação internacional para casos transfronteiriços cada vez mais comuns, e diferenciação entre usos legítimos e ilegítimos da tecnologia de síntese digital, mantendo lacunas estruturais que comprometem a efetividade de uma resposta regulatória sistemática.

A regulamentação eleitoral brasileira oferece o exemplo mais específico de tratamento dos deepfakes, com a Resolução TSE 23.732/2024 proibindo expressamente o uso de inteligência artificial para criar e propagar conteúdos falsos durante campanhas eleitorais. Esta medida, embora limitada ao contexto eleitoral, demonstra o reconhecimento institucional dos riscos específicos dos deepfakes e a necessidade de respostas normativas diferenciadas. Contudo, a fragmentação regulatória que trata deepfakes só em contextos setoriais específicos evidencia a ausência de abordagem sistemática e abrangente no Brasil.

O setor financeiro possui regulamentações do Banco Central sobre o uso de inteligência artificial em instituições financeiras, o setor de telecomunicações conta com normas da ANATEL sobre conteúdo digital e responsabilidade de provedores, o setor educacional dispõe de diretrizes do Ministério da Educação sobre implementação de IA em ambientes educacionais, e o setor de saúde possui regulamentações da ANVISA sobre dispositivos médicos que utilizam inteligência artificial. Esta multiplicidade de regulamentações setoriais, embora demonstre consciência institucional sobre os desafios da IA, cria inconsistências normativas, sobreposições de competências e lacunas regulatórias em áreas não especificamente contempladas, prejudicando a segurança jurídica e a efetividade das políticas públicas para enfrentamento dos riscos associados aos deepfakes.

2.4 O MODELO REGULATÓRIO FRANCÊS E A EXPERIÊNCIA EUROPEIA

A França desenvolveu uma das respostas legislativas mais avançadas aos desafios dos deepfakes, inserida no contexto normativo mais amplo da União Europeia. O marco regulatório francês, materializado principalmente na Lei SREN (*Sécuriser et Réguler l'Espace Numérique*) de 21 de maio de 2024, representa uma abordagem proativa que contrasta significativamente com a postura reativa observada no Brasil (FRANÇA, 2024). Esta legislação altera o Código Penal francês para incluir tipificação específica da criação e distribuição de deepfakes não consensuais, estabelecendo um regime jurídico autônomo que reconhece as particularidades técnicas e os danos únicos associados a esta tecnologia.

O contexto europeu é fundamental para compreender a abordagem francesa. O Ato Europeu de Inteligência Artificial (AI Act), que entrou em vigor em agosto de 2024, estabelece uma estrutura regulatória baseada em riscos que classifica os deepfakes como sistemas de alto risco quando utilizados para desinformação ou manipulação de processos democráticos (UNIÃO EUROPEIA, 2024). Este regulamento introduz obrigações específicas de rotulagem para conteúdo sintético, exigindo que sistemas de IA indiquem claramente quando conteúdo foi artificialmente gerado, medida que visa combater a

desinformação e proteger direitos individuais.

A Lei SREN francesa complementa o framework europeu com dispositivos nacionais específicos que criminalizam a criação e disseminação de deepfakes sem consentimento. A legislação estabelece distinções importantes entre diferentes tipos de uso, aplicando regimes jurídicos diferenciados conforme o contexto. Para deepfakes de natureza sexual não consensual, as penalidades são particularmente severas, refletindo o reconhecimento do impacto devastador deste tipo de conteúdo na vida das vítimas (HOGAN LOVELLS, 2024). A lei também estabelece exceções cuidadosamente delimitadas para fins artísticos, educacionais, jornalísticos e de sátira política, buscando equilibrar proteção contra abusos com preservação da liberdade de expressão e inovação tecnológica.

Um aspecto particularmente inovador da abordagem francesa é o regime de responsabilização proativa de plataformas digitais. Diferentemente do modelo brasileiro de "notice and take down" judicial, que exige ordem judicial específica para que plataformas removam conteúdo considerado ilícito, sistema que se caracteriza pela natureza reativa e procedimentos morosos que podem demandar semanas ou meses para conclusão, a legislação francesa estabelece que plataformas têm obrigações proativas de detectar e remover conteúdo sintético malicioso, não podendo limitar-se a uma postura reativa.

O modelo brasileiro tradicional, embora garanta maior segurança jurídica através do controle judicial, mostra-se inadequado para casos urgentes de deepfakes onde cada hora de permanência do conteúdo falso na rede pode amplificar exponencialmente os danos às vítimas. A recente evolução jurisprudencial do Supremo Tribunal Federal tem flexibilizado esta exigência de ordem judicial prévia para casos específicos, reconhecendo que plataformas possuem capacidade técnica para identificar conteúdos manifestamente ilícitos, criando precedentes importantes que aproximam o sistema brasileiro do modelo europeu de responsabilização proativa.

As plataformas francesas devem implementar sistemas de detecção automatizada, procedimentos de denúncia eficazes e mecanismos de remoção rápida, sendo passíveis de sanções administrativas em caso de descumprimento, modelo que contrasta com a nossa tradição de menor interferência estatal na moderação de conteúdo digital.

A implementação prática da legislação francesa tem revelado tanto sucessos quanto desafios. A jurisprudência francesa tem estabelecido precedentes importantes,

particularmente no reconhecimento de danos específicos causados por deepfakes e na determinação de responsabilidades solidárias de plataformas que se recusam a remover conteúdo prontamente. Um caso paradigmático envolveu deepfakes pornográficos de personalidade pública, onde o tribunal não apenas condenou criminalmente o criador do conteúdo, mas também estabeleceu responsabilidade da plataforma, criando precedente sobre responsabilização de intermediários tecnológicos (CIDADÃOS PELA CIBERSEGURANÇA, 2024).

O sistema francês também investe significativamente em capacitação técnica e jurídica, desenvolvendo programas de treinamento para magistrados, promotores e forças policiais visando aprimorar a compreensão técnica necessária para lidar com casos envolvendo deepfakes. Esta abordagem holística reconhece que a eficácia da regulamentação depende não apenas da existência de normas adequadas, mas da capacidade institucional para implementá-las adequadamente.

2.5 ANÁLISE COMPARATIVA E ADAPTAÇÕES PARA O CONTEXTO BRASILEIRO

A comparação entre os modelos francês e brasileiro revela diferenças fundamentais de abordagem regulatória que têm implicações diretas para a proteção de direitos fundamentais e a segurança jurídica. Enquanto a França adotou estratégia proativa baseada em legislação específica e responsabilização proativa de plataformas, o Brasil mantém abordagem reativa dependente de interpretações analógicas de normas pré-existentes. Esta diferença reflete filosofias distintas de regulação tecnológica: o modelo europeu de "regulação por antecipação" versus a tradição brasileira de "regulação por demanda" (MARTINS, 2024, p. 123-145).

A especificidade normativa constitui vantagem central do modelo francês. A Lei SREN estabelece definições claras de condutas proibidas, exceções permitidas e consequências jurídicas específicas para deepfakes, enquanto o Brasil depende de interpretações analógicas que geram incerteza jurídica tanto para potenciais infratores quanto para vítimas. A tipificação autônoma francesa oferece maior segurança jurídica e orienta mais claramente a ação de autoridades públicas, aspectos essenciais para efetividade da resposta regulatória (COSTA, 2023, p. 78-92).

Contudo, a experiência francesa não pode ser transplantada mecanicamente para o contexto brasileiro sem consideração das especificidades constitucionais, institucionais e

sociais nacionais. O sistema federativo brasileiro cria desafios de coordenação que não existem no sistema francês mais centralizado, exigindo articulação entre diferentes esferas de governo e órgãos competentes. Além disso, as diferenças econômicas e tecnológicas entre os países podem exigir adaptações nas obrigações impostas às plataformas digitais, considerando limitações de recursos e capacidade técnica das empresas que aqui operam.

O recente posicionamento do Supremo Tribunal Federal sobre responsabilização de plataformas digitais cria oportunidade única para aproximação do modelo brasileiro ao padrão francês. A formação de maioria no STF para ampliar a responsabilização independente de notificação judicial prévia representa evolução significativa que facilita a implementação de regime mais rigoroso especificamente para deepfakes. O reconhecimento de que plataformas possuem condições tecnológicas para detectar conteúdos ilícitos cria base jurisprudencial sólida para exigência de implementação de tecnologias de detecção de deepfakes (FERNANDES, 2024, p. 201-223).

Esta evolução jurisprudencial, combinada com crescente consciência sobre os riscos dos deepfakes evidenciada pelas regulamentações eleitorais e projetos de lei em tramitação, sugere momento propício para desenvolvimento de marco regulatório específico no Brasil. A adaptação da experiência francesa deve considerar elementos como a criação de tipificação penal autônoma para deepfakes maliciosos, estabelecimento de regime híbrido de responsabilização de plataformas que combine obrigações proativas para grandes plataformas com manutenção do sistema judicial para menores, e desenvolvimento de procedimentos específicos para casos urgentes envolvendo conteúdo sintético.

A proteção às vítimas representa área onde a experiência francesa oferece contribuições particularmente valiosas. O modelo francês de procedimentos expeditos para remoção de conteúdo, presunção de danos em casos de deepfakes de conteúdo sexual não consensual, e facilitação do acesso à justiça através de gratuidade automática em casos evidentes podem ser adaptados ao contexto brasileiro. Estas medidas são especialmente importantes considerando que os danos causados por deepfakes podem ser particularmente graves e duradouros, justificando proteções especiais que vão garantir o bem-estar e segurança, aos que estão convivendo em sociedade.

3. CONCLUSÃO

A presente pesquisa demonstrou que a experiência francesa na regulamentação de deepfakes oferece contribuições valiosas para o aperfeiçoamento do marco jurídico

brasileiro, especialmente considerando as recentes evoluções jurisprudenciais no Supremo Tribunal Federal. A análise comparativa revelou tanto convergências importantes quanto divergências significativas entre os sistemas jurídicos, permitindo identificação de elementos da experiência francesa que podem ser adaptados ao contexto brasileiro.

A França, beneficiando-se de sua inserção no contexto normativo da União Europeia, desenvolveu abordagem abrangente e tecnicamente sofisticada para regulamentação de deepfakes. O AI Act europeu estabeleceu precedente importante na regulamentação de inteligência artificial, criando obrigações específicas para sistemas que geram conteúdo sintético. A complementação deste framework com iniciativas nacionais francesas resultou em regime jurídico robusto e efetivo. O Brasil, por sua vez, encontra-se em momento de transição importante. O Marco Civil, embora pioneiro em sua época, mostrou limitações para lidar com desafios impostos por tecnologias emergentes como os deepfakes. Contudo, a evolução jurisprudencial recente do STF, particularmente no que se refere à responsabilização de plataformas digitais, cria oportunidades significativas para desenvolvimento de regulamentação mais efetiva. O ordenamento jurídico brasileiro, apesar de possuir marcos normativos avançados como o anteriormente mencionado, Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (Lei 13.709/2018), apresenta lacunas significativas no tratamento específico dos deepfakes. O Marco Civil, concebido em 2014 antes da popularização dos deepfakes e outras tecnologias de síntese digital, estabelece no artigo 19 um sistema de responsabilização de provedores que exige ordem judicial específica para remoção de conteúdo, modelo que se mostra inadequado para a natureza particularmente danosa e urgente dos casos envolvendo manipulação digital de imagem e voz. As limitações temporais da legislação evidenciam-se na ausência de previsões específicas para conteúdo sintético, uma vez que o foco normativo direcionou-se para conteúdo tradicional gerado por usuários humanos, não contemplando cenários de geração automatizada de material audiovisual falso.

As limitações procedimentais manifestam-se na inadequação dos prazos judiciais tradicionais para casos que exigem resposta imediata, na ausência de procedimentos expeditos específicos para conteúdo sintético e na falta de critérios jurídicos diferenciados para casos de manipulação digital que transcendem as categorias convencionais de conteúdo ilícito. As limitações técnicas revelam-se na inexistência de obrigações legais para implementação de sistemas de detecção automatizada de deepfakes, na ausência de requisitos técnicos para identificação e rotulagem de conteúdo sintético, e na falta de mecanismos sistematizados de cooperação internacional para enfrentamento de casos

transfronteiriços, aspectos fundamentais considerando a natureza global das plataformas digitais e a facilidade de disseminação internacional de deepfakes maliciosos.

As recomendações apresentadas buscam aproveitar esta janela de oportunidade, propondo adaptação de elementos da experiência francesa ao contexto constitucional e institucional brasileiro. A proposta de regime híbrido de responsabilização de plataformas, combinando elementos proativos para grandes plataformas com manutenção do sistema judicial para menores, representa o equilíbrio entre efetividade e direitos fundamentais.

A criminalização específica de condutas relacionadas ao uso malicioso de deepfakes, especialmente no contexto de conteúdo sexual não consensual e manipulação política, é essencial para proteção adequada dos direitos das vítimas. A experiência francesa demonstra que a tipificação específica, combinada com procedimentos expeditos e medidas de reparação adequadas, pode resultar em proteção mais efetiva. O investimento em capacitação técnica e desenvolvimento de tecnologias nacionais de detecção representa aspecto crucial para implementação efetiva de qualquer marco regulatório.

A coordenação institucional e a cooperação internacional também emergem como elementos fundamentais. A fragmentação de competências regulatórias no Brasil cria desafios significativos para a efetividade das políticas públicas de enfrentamento aos deepfakes, manifestando-se em múltiplas dimensões que comprometem a coerência e eficácia da resposta estatal. A fragmentação institucional caracteriza-se pela multiplicidade de órgãos reguladores com competências sobrepostas ou complementares, incluindo o TSE para questões eleitorais, a ANATEL para aspectos de telecomunicações, o Banco Central para questões financeiras, e diversos outros órgãos setoriais, sem que exista coordenação central específica para questões de inteligência artificial e deepfakes.

Esta ausência de coordenação central resulta em sobreposições de competências em alguns casos e lacunas regulatórias em áreas não especificamente contempladas por nenhum órgão, prejudicando a efetividade das políticas e criando incertezas jurisdicionais. A fragmentação normativa manifesta-se na coexistência de regulamentações setoriais frequentemente inconsistentes entre si, na ausência de princípios gerais unificadores que orientem a aplicação das normas específicas, e na dificuldade prática de aplicação em casos híbridos que envolvem múltiplos setores simultaneamente.

Os impactos negativos desta fragmentação incluem significativa insegurança jurídica para operadores econômicos e usuários, dificuldades de *enforcement* coordenado

que prejudicam a efetividade das sanções, possibilidades de conflitos normativos entre regulamentações setoriais divergentes, e comprometimento geral da efetividade das políticas públicas devido à falta de articulação institucional, evidenciando a necessidade de desenvolvimento de marco geral para inteligência artificial que unifique abordagens e estabeleça coordenação efetiva entre os diversos órgãos competentes.

É importante reconhecer que a regulamentação de deepfakes representa desafio complexo que exige equilíbrio cuidadoso entre diferentes valores e interesses. A proteção contra deepfakes maliciosos deve ser balanceada com preservação da liberdade de expressão, inovação tecnológica e viabilidade econômica das plataformas digitais. A experiência francesa oferece modelo de como este equilíbrio pode ser alcançado através de abordagem nuançada e tecnicamente informada.

O momento atual representa oportunidade única para o Brasil estabelecer-se como referência na regulamentação de tecnologias emergentes. A combinação de evolução jurisprudencial favorável, consciência crescente sobre os riscos dos deepfakes e disponibilidade de experiências internacionais cria condições ideais para desenvolvimento de marco regulatório avançado, embora seja fundamental que o processo se conduza de forma participativa e tecnicamente informada, com as especificidades do contexto brasileiro.

A pesquisa também revelou a importância de abordagem dinâmica e adaptativa para regulamentação de tecnologias emergentes. A rápida evolução dos deepfakes exige marcos regulatórios capazes de adaptação contínua, evitando obsolescência precoce das normas. Por fim, a experiência francesa demonstra que a regulamentação efetiva de deepfakes não é apenas possível, mas essencial para proteção de direitos fundamentais no ambiente digital contemporâneo. O Brasil possui todas as condições para desenvolvimento de regulamentação igualmente efetiva, desde que aproveite as lições da experiência internacional e as oportunidades criadas pela evolução jurisprudencial. O futuro da regulamentação de deepfakes no Brasil dependerá da capacidade de conjugar inovação jurídica com rigor técnico, proteção de direitos com preservação da inovação, e especificidade nacional com harmonização internacional. Assim, o sucesso final dependerá da capacidade brasileira de adaptação criativa e implementação efetiva.

4. REFERÊNCIAS

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Rio de Janeiro: Presidência da República, 1940.

ALVES, Fernando de Brito; KAZMIERCZAK, Luiz Fernando. O Direito Penal Diante da Sociedade de Risco: A Criminalização Motivada pelo Medo. *CONPEDI Law Review*, Uruguai, v. 2, n. 4, p. 36-57, jul./dez. 2016.

BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. 2. ed. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Senado Federal. **Projeto de Lei nº 146/2024**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para agravar a pena dos crimes contra a honra quando praticados por meio de deepfake. Brasília: Senado Federal, 2024a.

BRASIL. Tribunal Superior Eleitoral. **Resolução TSE nº 23.732/2024**. Dispõe sobre atos preparatórios, registro de candidaturas, propaganda eleitoral, prestação de contas e diplomação nas eleições. Brasília: TSE, 2024b.

CHESNEY, Robert; CITRON, Danielle. **Deep Fakes: a looming challenge for privacy, democracy, and national security**. *California Law Review*, v. 107, n. 6, p. 1753-1820, 2019.

CIDADÃOS PELA CIBERSEGURANÇA. **Prevenção de Deepfakes: Urgência Legislativa em Portugal e na União Europeia**. 2024. Disponível em: <https://cidadaospelaciberseguranca.com/2024/05/29/prevencao-de-deepfakes-urgencia-legislativa-em-portugal-e-na-uniao-europeia/>. Acesso em: 30 jan. 2025.

COSTA, Maria Silva. **Deepfakes e Direito Penal: desafios da era digital**. São Paulo: Revista de Direito Digital, v. 15, n. 3, p. 78-92, 2023.

FERNANDES, João Pedro. **Inteligência Artificial e Direitos Fundamentais**. Rio de Janeiro: Editora Jurídica, p. 201-223, 2024.

FRANÇA. **Lei SREN (Sécuriser et Réguler l'Espace Numérique)**. Lei nº 2024-449, de 21 de maio de 2024. Paris: Journal Officiel, 2024.

HOGAN LOVELLS. **France prohibits non-consensual deep fakes**. 2024. Disponível em: <https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes>. Acesso em: 2 jun. 2025.

LIBRARY OF CONGRESS. **France: Bill Introduced to Require Labeling of AI-Generated Images on Social Networks**. 2025. Disponível em: <https://www.loc.gov/item/global-legal-monitor/2025-03-07/france-bill-introduced-to-require-labeling-of-ai-generated-images-on-social-networks/>. Acesso em: 15 set. 2024.

MARTINS, Ana Carolina. **Direito Comparado e Tecnologia**. Brasília: Editora UnB, p. 123-145, 2024.

PEREIRA, Carlos Eduardo. **Cooperação Internacional em Direito Digital**. São Paulo: Revista Brasileira de Direito Internacional, v. 12, n. 2, p. 156-178, 2023.

RÖSSLER, Beate. **The Value of Privacy in the Digital Age**. Journal of Moral Philosophy, v. 18, n. 1, p. 45-67, 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho relativo à harmonização das regras sobre inteligência artificial (Ato da IA)**. Jornal Oficial da União Europeia, L 1689, 12 jul. 2024.

VACCARI, Cristian; CHADWICK, Andrew. **Deepfakes and Disinformation: Exploring how Citizens Think about Synthetic Political Videos**. Journalism Studies, v. 21, n. 17, p. 2395-2412, 2020