


Artigos Científicos

Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital

Deep fake, personality rights and criminal law: an analysis of technological impacts in the digital age

Giovanna Aleixo Gonçalves Oliveira , Gustavo Noronha de Ávila 

¹Centro Universitário Cesumar , Maringá, RS, Brasil

RESUMO

A tecnologia trouxe mudanças significativas para a sociedade, e uma dessas inovações, conhecida como Deep Fake, ganha destaque nas discussões contemporâneas. Termo esse que é associado a técnica de fusão de imagem em movimento com uma voz em situações que não ocorreram. Este artigo tem como objetivo analisar os impactos da tecnologia Deep Fake no contexto dos direitos da personalidade e do Direito Penal. Com o advento da era digital, a criação de vídeos e áudios sintéticos hiper-realistas tem levantado questões éticas, legais e sociais. Neste cenário, é fundamental compreender como a tecnologia Deep Fake afeta direitos fundamentais, como a privacidade, a imagem e a reputação das pessoas, bem como o Direito Penal lida com esse fenômeno. O estudo abordará os conceitos e a evolução da tecnologia Deep Fake, examinando casos emblemáticos de seu uso indevido. Além disso, investigará as implicações nos direitos da personalidade, destacando a necessidade de adaptação do Direito Penal para enfrentar essa nova ameaça. A metodologia utilizada foi a hipotético-dedutiva, por meio do método teórico-bibliográfico, com coletas de dados realizados em sites de busca acadêmica, bibliotecas e revistas científicas que abordam a temática. Por fim, o artigo irá propor recomendações e soluções para proteger os indivíduos contra os abusos da tecnologia Deep Fake e garantir a preservação dos direitos da personalidade na era digital.

Palavras-chave: Deep Fake; Direitos da Personalidade; Direito Penal; Tecnologia; Privacidade, Ética

ABSTRACT

Technology has brought significant changes to society, and one of these innovations, known as Deep Fake, is highlighted in contemporary discussions. This term is associated with the technique of fusing a moving image with a voice in situations that did not occur. This article aims to analyze the impacts of Deep Fake technology in the context of personality rights and Criminal Law. With the advent of the digital era, the creation of hyper-realistic synthetic videos and audio has raised ethical, legal and social

questions. In this scenario, it is essential to understand how Deep Fake technology affects fundamental rights, such as people's privacy, image and reputation, as well as how Criminal Law deals with this phenomenon. The study will address the concepts and evolution of Deep Fake technology, examining emblematic cases of its misuse. Furthermore, it will investigate the implications for personality rights, highlighting the need to adapt Criminal Law to face this new threat. The methodology used was hypothetical-deductive, through the theoretical-bibliographic method, with data collection carried out on academic search websites, libraries and scientific journals that address the topic. Finally, the article will propose recommendations and solutions to protect individuals against the abuse of Deep Fake technology and ensure the preservation of personality rights in the digital age.

Keywords: Deep Fake; Personality Rights; Criminal Law; Technology; Privacy, Ethics

RESUMEN

La tecnología ha traído cambios significativos a la sociedad y una de estas innovaciones, conocida como Deep Fake, se destaca en los debates contemporáneos. Este término está asociado a la técnica de fusionar una imagen en movimiento con una voz en situaciones que no ocurrieron. Este artículo tiene como objetivo analizar los impactos de la tecnología Deep Fake en el contexto de los derechos de la personalidad y el Derecho Penal. Con el advenimiento de la era digital, la creación de videos y audios sintéticos hiperrealistas ha planteado cuestiones éticas, legales y sociales. En este escenario, resulta fundamental entender cómo la tecnología Deep Fake afecta a derechos fundamentales, como la privacidad, la imagen y la reputación de las personas, así como cómo el Derecho Penal aborda este fenómeno. El estudio abordará los conceptos y la evolución de la tecnología Deep Fake, examinando casos emblemáticos de su mal uso. Además, se investigarán las implicaciones para los derechos de la personalidad, destacando la necesidad de adaptar el Derecho Penal para afrontar esta nueva amenaza. La metodología utilizada fue hipotético-deductiva, a través del método teórico-bibliográfico, realizándose la recolección de datos en sitios web de búsqueda académica, bibliotecas y revistas científicas que abordan el tema. Finalmente, el artículo propondrá recomendaciones y soluciones para proteger a las personas contra el abuso de la tecnología Deep Fake y garantizar la preservación de los derechos de la personalidad en la era digital.

Palabras-Clave: Deep Fake; Derechos de la Personalidad; Derecho penal; Tecnología; Privacidad, Ética

1 INTRODUÇÃO

O avanço tecnológico tem revolucionado muitos aspectos da sociedade, trazendo consigo benefícios significativos, mas também desafios complexos. Uma dessas inovações tecnológicas que tem chamado a atenção é a tecnologia conhecida como *Deep Fake*¹, a qual permite a criação de vídeos e áudios sintéticos que se assemelham de maneira impressionante a um conteúdo real, muitas vezes com o uso de inteligência artificial.

¹ Tradução livre: "junção do termo "deep learning" (aprendizagem profunda em inglês) e "fake" (falso em inglês), é uma técnica de síntese de imagens ou sons humanos baseada em inteligência artificial"

Embora a tecnologia *Deep Fake* tenha aplicações legítimas, como na indústria cinematográfica e publicitária, ela também tem sido usada indevidamente para criar conteúdo enganoso, difamatório e até mesmo pornográfico, envolvendo pessoas que muitas vezes não têm conhecimento ou consentimento para tal uso. Esse uso indevido pode ferir o direito personalíssimo do indivíduo, como seu direito a imagem

Neste contexto, surge uma questão crucial para a sociedade e para o campo do Direito: como a tecnologia *Deep Fake* afeta os direitos da personalidade e como o Direito Penal pode lidar eficazmente com essa nova ameaça à dignidade humana e à integridade pessoal? O presente artigo irá debater sobre essa problemática enfrentada nos dias atuais.

Este artigo tem como objetivo analisar esses impactos, explorando os conceitos da tecnologia *Deep Fake*, examinando sua relação com os direitos da personalidade e discutindo como o Direito Penal pode responder a esse desafio.

2 A TECNOLOGIA DEEP FAKE: CONCEITOS E EVOLUÇÃO

O conceito de *Deep Fake* e Inteligência Artificial estão interligados, visto que, para este estudo se mostra necessário compreender a inteligência artificial como uma área dentro da ciência da computação, e conseqüentemente o campo do *Machine Learning*² e *Deep Learning*³, que somados com as "*Fake News*"⁴ gera o termo "*Deep fake*".

Muitas são as definições para a Inteligência Artificial, dentre elas temos a definição trazida por Ruy Flávio, que afirma que a inteligência artificial seria ações comparadas as ações humanas, entretanto afirma que muitas vezes a máquina não consegue traduzir exatamente um comportamento Inteligente, podendo errar, mesmo sendo programada para não:

É o conjunto de ações que, se fossem realizadas por um ser humano, seriam consideradas inteligentes. É uma definição que nos chama a comparar as ações dos computadores com as nossas próprias para definirmos se estamos diante

² Machine Learning é uma área da Inteligência Artificial e da ciência da computação que usa dos dados e algoritmos para imitar a maneira como os humanos aprendem.

³ Deep Learning baseia-se em um conjunto de algoritmos relacionados ao machine learning

⁴ Tradução livre: junção do termo fake (falso) e news (notícia), ou seja, notícias falsas

de um comportamento inteligente ou não. Em que pese ser uma definição útil, não é de todo precisa, uma vez que há algumas ações que o computador consegue realizar que não traduzem adequadamente um comportamento inteligente⁵.

Para Rosa⁶, a inteligência Artificial (IA) é a capacidade que os computadores possuem de realizar tarefas que só os próprios seres humanos realizam, ou seja, quando o computador realiza alguma tarefa que o ser humano comum poderia realizar.

Dentro de uma subárea da IA se encontra o *Machine Learning*, que possui como base a estatística computacional e procedimentos de otimização, buscando técnicas de aprendizado para possíveis soluções de problemas ou tarefas específicas. Conforme Damaceno e Vasconcellos, os algoritmos de *Machine Learning* possuem equações pré-definidas para execução de acordo com a demanda, e como por exemplo, o uso de *Machine Learning* na identificação de spams⁷.

Dentro da subárea *Machine Learning* encontra-se a *Deep Learning*, que tem como função capacitar a máquina para a realização de tarefas mais complexas, estabelecendo parâmetros sobre dados, treinando o computador para aprender com o uso de processamento no reconhecimento de padrões.⁸

Partindo do *Deep Learning* tem-se o termo *Deep Fakes*, que são criações audiovisuais geradas por algoritmos de aprendizado profundo, que utilizam dados e referências para produzir conteúdo visual e auditivo que pode ser extremamente difícil de distinguir da realidade. Essa tecnologia evoluiu consideravelmente ao longo dos anos, tornando-se cada vez mais acessível e convincente. O termo *Deep Fake* junta os termos *Deep learning* (aprendizagem profunda em inglês) e Fake (que quer dizer falso).

Do mesmo modo Battaglia aduz que:

Os *deep fakes* nada mais são do que vídeos criados a partir de inteligência artificial e que reproduzem a aparência, as expressões e até a voz de

⁵ Oliveira, Ruy Flávio de. *Inteligência Artificial*. Londrina: Editora e Distribuidora Educacional S.A, 2018, p. 10.

⁶ Rosa, João Luís Gracia. *Fundamentos da Inteligência Artificial*. Rio de Janeiro: LTC, 2011, p. 3.

⁷ Damaceno, Siuari Santos. Vasconcelos, Rafael Oliveira. *Inteligência Artificial: Uma breve abordagem sobre seu conceito real e o conhecimento popular*. Ciências exatas e tecnológicas. Aracaju. v. 5, n.1, 2018, p. 11-16.

SPAM é um termo que faz referência direta a e-mails indesejados, e comportamentos em redes sociais pra propagar notícias falsas.

⁸ Damaceno, Siuari Santos. Vasconcelos, Rafael Oliveira. *Inteligência Artificial: Uma breve abordagem sobre seu conceito real e o conhecimento popular*. Ciências exatas e tecnológicas. Aracaju. v. 5, n.1, p. 11-16, 2018.

alguém do mundo real. O nome vem da junção de duas expressões em inglês: “*deep learning*” (“aprendizado profundo”) e “*fake*” (“falso”).⁹

Spencer descreve como as *deep fakes* são geradas a partir de inteligência artificial:

Deep fakes são, essencialmente, identidades falsas criadas com o *Deep Learning* [aprendizagem profunda, por meio de uso maciço de dados], por meio de uma técnica de síntese de imagem humana baseada na inteligência artificial. É usada para combinar e sobrepor imagens e vídeos preexistentes e transformá-los em imagens ou vídeos “originais” [...] Essa combinação de vídeos existentes e “originais” resulta em vídeos falsos, que mostram uma ou algumas pessoas realizando ações ou fazendo coisas que nunca aconteceram na realidade. Em 2019, também estamos vendo uma explosão de faces *fake*, através das quais a IA é capaz de conjurar pessoas que não existem na realidade, e que têm um certo fator de fluência.¹⁰

Alguns exemplos de *deep fake* surgiram nas redes sociais, nas quais os primeiros casos começaram com cunho pornográfico, o que mais tarde evoluiu para outros intuitos danosos, como nas eleições, onde pode-se citar o vídeo do ex-presidente dos Estados Unidos, Barack Obama, fazendo críticas à Donald Trump.

A tecnologia *Deep Fake* evoluiu rapidamente desde sua criação. Inicialmente, esses vídeos sintéticos eram usados principalmente para criar paródias e conteúdo humorístico. No entanto, à medida que a tecnologia se tornou mais sofisticada, seu uso indevido se disseminou.

É possível perceber que a história da Inteligência artificial se confunde com a da computação. Depois do surgimento do primeiro computador iniciou uma corrida com objetivo de criar máquinas cada vez melhores para utilizar em guerras. Um dos primeiros grandes trabalhos envolvendo Inteligência Artificial foi feito por Warren Mcculloch e Walter Pitts, em 1943. Mcculloch e Pitts que se basearam em três fontes para a criação, sendo elas; o conhecimento básico de fisiologia, a função dos neurônios

⁹ Battaglia, Rafael. Afinal, o que são deepfakes?2020. Disponível em: <https://super.abril.com.br/tecnologia/afinal-o-que-sao-deepfakes/>. Acesso: 22 set. 2023.

¹⁰ Spencer, Michael K. Deep Fake, a mais recente ameaça distópica. Tradução de Gabriela Leite. Disponível em: <https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/>. Acesso em: 22 set. 2023.

no cérebro, a lógica proposicional e a teoria da computação de Turing¹¹; resultando em um modelo de neurônios artificiais.¹²¹³

No ano de 1969, a Universidade de Stanford desenvolveu um programa denominado Dendral¹⁴, com objetivo de desenvolver soluções capazes de encontrar moléculas orgânicas¹⁵. Esse programa foi importante na história da Inteligência Artificial, a partir daí se desenvolveram programas inteligentes.

Nos anos seguintes foram feitas várias pesquisas, trazendo uma grande evolução no campo da IA. A partir da década de 1990 é o período na qual as pesquisas saíram das universidades e chegaram nas empresas.

Hoje, as *Deep Fakes* podem ser usadas para criar vídeos e áudios extremamente realistas de indivíduos, muitas vezes sem seu consentimento. Em 2022, no ano eleitoral, a *Deep Fake* foi usada como ferramenta de manipulação política, apontada aqui com uma ação grave diante do indivíduo. Na era da *Fake News* a *deep fake* é uma ferramenta poderosa para disseminar a desinformação, podendo ferir direitos inatos ao ser humano, conforme se verá a seguir.

3 IMPACTOS NOS DIREITOS DA PERSONALIDADE: DA PRIVACIDADE, IMAGEM E REPUTAÇÃO DO INDIVÍDUO

Conforme Maicá¹⁶ as mudanças trazidas com o uso das tecnologias digitais fizeram a sociedade se reinventar, ressignificando o que se entende por vida privada e intimidade. O autor explica o surgimento do direito à privacidade:

¹¹ A teoria de Alan Turing propunha a construção de uma máquina universal capaz de operar com uma sequência de instruções e dados entremeados em uma fita de comprimento infinito.

¹² Um neurônio artificial representa a base de uma rede neural artificial, um modelo da neurocomputação e orientado nas redes neurais biológicas.

¹³ Gomes, Denis dos Santos. Inteligência artificial. Conceitos e Aplicações. Revista Olhar Científico. Faculdades Associadas de Ariquemes –V. 01, n.2, Ago./Dez., 2010, p. 3.

¹⁴ Dendral é um sistema especialista e um projeto pioneiro em inteligência artificial, que começou a ser desenvolvido em 1965, na Universidade de Stanford.

¹⁵ Moléculas orgânicas de acordo com o programa Dendral são as informações usadas pelo programa

¹⁶ MAICÁ, Richard da Silveira. Direito fundamental à privacidade: desdobramentos possíveis até o direito à intimidade. Dissertação de Mestrado em Direito pelo Programa de Pós Graduação da Universidade Federal de Santa Maria. 2018. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/20151/DIS_PPGDIREITO_2017_MAICA_RICHARD.pdf?sequence=1&isAllowed=y. Acesso em: 05 out. 2022.

A base teórica que sustentou o surgimento do direito à privacidade pode ser entendida com base no fato de o indivíduo ter a opção de revelar informações a seu respeito ou não, permitindo a manutenção na própria vida e no próprio domicílio. Logo, o campo de proteção da privacidade objetiva evitar intromissões indesejadas nas informações em que o indivíduo não desejasse que se tornassem públicas.

Nessa linha, a Constituição Federal de 1988 traz os direitos à personalidade como direitos essenciais à dignidade e integridade, independentemente de capacidade civil. O artigo 5º, inciso X, da Constituição¹⁷ traz a intimidade e a vida privada como direitos invioláveis:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

No Brasil, a Lei Geral de Proteção de Dados (Lei. 13.709/18)¹⁸ foi a responsável por trazer o respeito a privacidade, a inviolabilidade da intimidade, da honra e da imagem. Ela surge com o objetivo de promover o desenvolvimento econômico e tecnológico das empresas, e a de proteger direitos e liberdades fundamentais dos titulares.

Pode-se perceber que se vive em uma época de hiperexposição¹⁹, podendo ser voluntária ou não. Quando esta exposição é utilizada com má-fé, valendo-se de dados sensíveis de um terceiro, tem-se a evidência clara da violação dos direitos dos cidadãos quanto a sua privacidade. Segundo Ávila²⁰:

A hiperexposição está ligada ao uso compulsivo das mídias sociais, expondo a vida cotidiana, sem levar em conta os riscos que podem causar, bem como a segurança da rede. Inicia-se o uso por um hábito de informar e acaba por um vício em se expor. Entre as tecnologias digitais que impulsionam os hábitos descritos anteriormente, o smartphone é a principal, vez que converge a

¹⁷ BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

¹⁸ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 fev. 2024.

¹⁹ Hiperexposição é a grande exposição nas mídias sociais, se tornando muitas vezes um vício em expor.

²⁰ Ávila, G. N.; Corazza, T. A. M. . A HIPEREXPOSIÇÃO PESSOAL E SEUS REFLEXOS NOS DIREITOS DA PERSONALIDADE: NECESSIDADE DE UMA TUTELA TRANSVERSAL DO DIREITO À PRIVACIDADE, COM ENFOQUE NO ÂMBITO PENAL. JURIS POIESIS, v. 25, p. 144-177, 2022.

informação em tempo real, a exposição, a conexão, o uso da tecnologia e o *multitasking*²¹.

De acordo com Bolesina e Gervasoni²² o direito à privacidade é atualmente um dos mais diluídos, ou seja, sua proteção alcança diversos âmbitos, como integridade física, dados pessoais, autonomia e propriedade privada.

A privacidade das pessoas está sendo ameaçada pela capacidade de criar vídeos *Deep Fake* que retratam indivíduos em situações falsas e comprometedoras. A disseminação desse conteúdo pode causar danos significativos à reputação e à vida pessoal das pessoas envolvidas.

O direito a imagem é assegurado pela Constituição Federal em seu artigo 5º, X²³; pelo Código Civil em seu artigo 11²⁴ e 20²⁵ e pelo Código Penal em seu artigo 218-C²⁶. Sendo considerado um direito personalíssimo do indivíduo, conferindo a pessoa a faculdade de usar a própria imagem, dispor dela e reproduzi-la, podendo ter caráter comercial ou não. Nesse sentido entende-se que o direito à imagem protege principalmente interesses existenciais da pessoa, sendo considerado direito da personalidade por estar ligado ao indivíduo na condição de ser.

Por ser um direito personalíssimo tem-se um rol de mecanismos para sua proteção, sendo os principais a tutela inibitória, tutela reparatória e tutela preventiva, sendo aplicadas de acordo com cada caso que trate de dano à imagem.

²¹ Tradução livre: multitarefa, conceito usado para uma pessoa que faz duas ou mais atividades ao mesmo tempo

²² Bolesina, Iuri; Gevarsoni, Tássia. A Proteção do Direito Fundamental à Privacidade na Era Digital e a Responsabilidade Civil por Violação ao Direito à Intimidade. Revista Novos Estudos Jurídicos - Eletrônica, Vol. 27, N. 1, 2022. Disponível em: <https://periodicos.univali.br/index.php/nej/article/view/16093/10742>. Acesso em 20 set. 2023.

²³ Art. 5º Todos são iguais perante a Lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

²⁴ Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

²⁵ Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

²⁶ Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: (Incluído pela Lei nº 13.718, de 2018) Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

A tutela preventiva do ilícito, tem como objetivo impedir a prática do mesmo e inibir a repetição ou a continuação dessa prática, sendo esta tutela muito utilizada nos casos em que envolve o âmbito digital. A injusta violação deste direito gera consequência o dever de compensar o dano moral sofrido pela vítima, sendo aplicadas as penas de indenização em casos comprovados em que a utilização da imagem trouxe prejuízo material ou financeiro.

A criação de *Deep Fakes* que retratam os indivíduos de maneira difamatória ou prejudicial pode afetar seriamente sua imagem e reputação, muitas vezes causando danos irreparáveis. Visto que se trata de um conteúdo com alto poder de compartilhamento, como foi o caso das *deep fakes* usadas nas eleições, onde um vídeo do Jornal Nacional adulterado mostrando as intenções de votos nas eleições presidenciais gerou violação a toda a sociedade com a disseminação de notícias falsas.

Nesse sentido, deve-se ter o consentimento expresso da pessoa, consentimento este que caso seu contexto seja alterado deverá ser revalidado²⁷. Em voto, o Ministro Raul Araújo enfatizou a importância do consentimento expresso para a utilização da imagem humana em quadro televisivo:

“[...] não obstante o direito de informação da empresa de comunicação e o perceptível caráter de interesse público do quadro retratado no programa televisivo, está clara a ofensa ao direito à imagem do recorrido, pela utilização econômica desta, sem a proteção dos recursos de editoração de voz e de imagem para ocultar a pessoa, evitando-se a perfeita identificação do entrevistado, à revelia de autorização expressa deste, o que constitui ato ilícito indenizável. 3. A obrigação de reparação decorre do próprio uso indevido do direito personalíssimo, não sendo devido exigir-se a prova da existência de prejuízo ou dano. O dano é a própria utilização indevida da imagem”²⁸.

²⁷ Diante da ausência de uma lei específica para a proteção de dados pessoais, no Brasil foi positivada no Marco Civil da Internet (BRASIL, 2014), uma série de direitos essenciais para o usuário da rede, a partir da perspectiva do controle e da autodeterminação informativa. Foram observados também os princípios consagrados pela doutrina para a proteção dos dados pessoais, tais como a finalidade da coleta dos dados, a pertinência e a utilização não abusiva. Tal preocupação coaduna-se com a atual evolução do cenário tecnológico, em que se discute a utilização do Big Data, conjunto de soluções tecnológicas capaz de lidar com dados digitais em volume, variedade e velocidade até então inéditos. No artigo 7º desta Lei, encontra-se disposto que ao usuário são assegurados direitos, como o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (VII), e o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (IX). Portanto, o consentimento nessa lei é qualificado como livre, expresso e informado.

²⁸ Superior Tribunal de Justiça. Recurso especial n. 794586/RJ. Relator: Min. Raul Araújo. Diário da Justiça eletrônico, 21 mar. 2012a

É importante frisar que o artigo 21 do Marco Civil da Internet²⁹ cita a chamada pornografia da vingança, mas não somente ela, o legislador traz casos de por exemplo *hackers* que ameacem divulgar imagens de terceiros se não receberem algum tipo de vantagem econômica. Assim conclui, o direito a imagem é um direito de difícil garantia nos dias atuais, entretanto de grande importância, visto que se trata de direito personalíssimo. O Brasil e o mundo ainda estão correndo para a proteção efetiva desse direito, entretanto o rápido avanço da internet traz uma dificuldade.

4 O DIREITO PENAL E OS DESAFIOS DAS DEEP FAKES

O Direito Penal muitas vezes não está equipado para lidar com os casos *envolvendo Deep Fakes*, uma vez que as leis atuais nem sempre abrangem esse tipo de atividade criminosa. Isso cria lacunas legais que podem ser exploradas por criminosos.

Uma das primeiras convenções que abordou cibercrime foi a Convenção de Budapeste³⁰, esta convenção foi firmada em 2001 onde as autoridades brasileiras passaram a ter mais recursos para a investigação de crimes cibernéticos, ela é considerada um marco importante na luta contra os crimes cometidos no ambiente virtual em todo mundo, após sua implementação foi possível garantir a segurança e a privacidade do usuário da internet.

Tem-se ainda o Tratado Internacional de Direito Penal e Direito Processual Penal, em vigor desde 2004, criado com objetivo de colaboração no combate aos crimes praticados na rede mundial de computadores. O Brasil não aderiu a esse Tratado, assim em 2013 passou a vigorar as Leis 12.737/2012 conhecida como Lei Carolina

²⁹ Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

³⁰ CONVENÇÃO DE BUDAPESTE SOBRE A CIBERCRIMINALIDADE. 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 20 fev. 2024.

Dieckman³¹, e a 12.735/2012 conhecida como Lei Azeredo, sendo as primeiras tipificações criminais sobre crimes de informática no Brasil, possibilitando a responsabilização criminal, trazendo mais tarde os artigos 154-A³² e o 154-B³³, e alterações nos artigos 266³⁴ e 298³⁵ do Código Penal brasileiro.

Anos depois tivemos o que é considerado o maior marco na regulamentação de crimes digitais, que foi a Lei Federal nº 12.965/2014³⁶, conhecida como Marco Civil da Internet, que regula o uso da internet no Brasil, trazendo princípios, garantias, direitos e deveres para quem usa a rede.

Em 2018, o Brasil promulgou a lei federal nº 13.709/2018 que objetiva proteger e tratar os dados nos meios digitais, realizados por empresas; tendo como principal foco os dados sensíveis de cada pessoa.

Entretanto não se tem um tipo penal específico para *Deep fakes*, resultando em brechas para que os responsáveis pelos atos não sejam punidos. Para Mendonça e Rodrigues as *deep fakes* são problemas novos na sociedade, assim afirma:

Trata-se, assim, de um problema novo, que ainda precisa ser encarado de forma mais detida pela doutrina e, sobretudo, pela sociedade civil, pautando-se o debate pela inafastável certeza de que a educação digital das pessoas tem o

³¹ BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Define crimes cibernéticos e dá outras providências. Diário Oficial da União, Brasília, DF, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 fev. 2024.

³² Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. BRASIL. Lei Nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 set. 2023

³³ Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

³⁴ Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. BRASIL. Lei Nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 21 set. 2023

³⁵ Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. BRASIL. Lei Nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 21 set. 2023

³⁶ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 set. 2023

poder de contribuir para diminuir os impactos da desinformação e da circulação de imagens manipuladas.³⁷

Percebe-se assim uma dificuldade com esses tipos de crimes, e sua falta de legislação específica.

A *deep fakes* se popularizou a partir do uso de imagens de famosos alteradas, na maioria das vezes com citação cômica resultando em uma popularização na internet. O auge dela foi em 2017 quando circulou em grande quantidade *deep fakes* pornográficas, anos depois voltou a intensificar o uso com a tensão política no Brasil, momento em que se espalhou diversas informações falsas sobre as eleições.

Atualmente contamos com técnicas avançadas para detectar *deep fakes*, sendo a ciência forense uma das aliadas, como por exemplo o exame de vídeos adulterados para encontrar inconsistências, como o piscar dos olhos; como a pessoa do vídeo fala, analisando se o áudio e o movimento da boca se encaixam; a pele da pessoa do vídeo ou foto; o uso de óculos também é um grande aliado, visto que pode ser analisado o ângulo e a iluminação do mesmo; os pelos faciais e o tamanho e cor dos lábios também são pontos importantes para análise.

A *deep fakes* permite todos os tipos de fraudes, incluindo manipulação dos processos democráticos e dos sistemas judiciários e científicos. Resultando em uma maior desconfiança daqueles que trabalham com conteúdos digitais

A capacidade de criar *deep fakes* como provas em processos judiciais levanta preocupações sérias sobre a integridade do sistema de justiça criminal. Como os tribunais podem distinguir entre provas genuínas e *deep fakes*.

5 ADAPTAÇÕES NECESSÁRIAS E SOLUÇÕES

A criação de legislação específica para abordar crimes relacionados a *deep fakes* é fundamental, podendo incluir penalidades mais severas para a criação e disseminação indevida de *deep fakes*.

³⁷ Mendonça, Helena C. F. Coelho; Rodrigues, Paula Marques. Deepfakenews e sua influência no universo feminino. Migalhas, 4 jul. 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16, MI282987,31047Deep+fake+news+e+sua+influencia+no+universo+feminino>>. Acesso em: 21 set. 2023

As legislações existentes ainda que busquem se adequar as *deep fakes* não conseguem atingir seu objetivo.

Mendonça e Rodrigues corroboram que:

Uma alternativa para o combate de (Deep) Fake news seria “a criação de um algoritmo capaz de detectar o que é ou não Fake news, mas obviamente isso geraria ainda mais críticas. Quem controla a caixa-preta do algoritmo e determina os parâmetros do que é falso ou verdadeiro?”³⁸

Porém existem dificuldades em imputar às plataformas a responsabilidade pelas divulgações de *deep fakes*. De acordo com Agnoletto e Bezerra já existem algumas técnicas para identificação de *deep fakes*³⁹, como por exemplo o caso da XceptionNet, desenvolvida pela Technical University of Munich, essa técnica:

Trata-se de um algoritmo de aprendizagem profunda que identifica vídeos cujos rostos foram substituídos por outros. Os pesquisadores coletaram mais de mil vídeos cujos rostos foram substituídos e também os vídeos originais e criaram um banco de dados com mais de meio milhão de imagens de rostos alterados. A partir disto, criaram um banco de dados de rostos manipulados de FaceForensics e utilizaram um modelo de rede neural de aprendizagem profunda para compreender a diferença entre o vídeo real e o vídeo modificado. A partir deste projeto criaram o algoritmo denominado XceptionNet que representa uma importante solução para identificar vídeos que sofreram manipulação facial e outras alterações.⁴⁰

Assim o algoritmo denominado *XceptionNet* usa a técnica de aprendizagem *Machine learning* para reconhecer quando o vídeo é real e quando é manipulado, usando como base diversos vídeos de diferentes ângulos.

Especialistas afirmam que medidas legislativas são possibilidades de combate, entretanto essa medida poderia afetar diretamente os direitos fundamentais dos cidadãos, como liberdade de expressão e da informação. Entretanto para Siqueira⁴¹ a proteção da imagem e combate a *deep fakes* só será efetiva quando o Brasil aderir a

³⁸ Mendonça, Helena C. F. Coelho; Rodrigues, Paula Marques. Deepfakenews e sua influência no universo feminino. Migalhas, 4 jul. 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16, MI282987,31047Deep+fake+news+e+sua+influência+no+universo+feminino>. Acesso em: 23 set. 20213.

³⁹ Bezerra, Calyton da Silva, Agnoletto, Giovanni Celso. Combate às Fake News/ organizador: Clayton da Silva Bezerra / Giovanni Celso Agnoletto 1 ed. -São Paulo: Editora Posteridade, 2019, p. 126.

⁴⁰ Bezerra, Calyton da Silva, Agnoletto, Giovanni Celso. Combate às Fake News/ organizador: Clayton da Silva Bezerra / Giovanni Celso Agnoletto 1 ed. -São Paulo: Editora Posteridade, 2019, p. 126

⁴¹ Siqueira, Paulo Alexandre Rodrigues de. O 'Deep Fake' e a Legislação Brasileira -utilização de instrumentos legais para a proteção à imagem Conteúdo Jurídico, Brasília-DF: 29 set 2021. Disponível em:<https://conteudojuridico.com.br/consulta/artigo/53256/o-deep-fake-e-a-legislao-brasileira-utilizao-deinstrumentos-legais-para-a-proteo-imagem>. Acesso em: 20 set. 2020.

Convenção de Budapeste, que abrirá espaço para a criação de políticas criminais objetivando a proteção da sociedade.

Embora não se tenha legislação específica para os casos de *deep fake* o Marco Civil da Internet trouxe muitas mudanças, ele traz um contexto regulatório que promove a privacidade e a liberdade de expressão online, o que pode beneficiar a forma como as pessoas utilizam e protegem suas imagens pessoais na era digital.

Alguns dos benefícios indiretos trazidos pela Lei nº 12.965/2014⁴², popularmente conhecida como Marco Civil da Internet é a neutralidade da rede, que garante que os provedores de internet não devem discriminar ou favorecer determinados conteúdos, assegurando que todos tenham acesso igualitário à internet e permitindo que as pessoas compartilhem e acessem informações, imagens sem discriminação. Outro ponto que a Lei traz é a proteção à privacidade, relacionando os princípios de privacidade, ajudando na proteção das pessoas no ambiente online, incluindo a proteção de sua imagem pessoal contra o uso não autorizado. A proteção à privacidade é o que a lei mais protege contra as *deep fakes*, visto que esse ato criminoso é feito com o uso indevido da imagem da pessoa, ferindo principalmente sua privacidade.

Citamos ainda a Transparência e Informação, a lei traz a importância da transparência e informação sobre políticas de privacidade e termos de uso, ora nada mais é do que a ciência de que na internet existem regras, assim como nos demais espaços, entretanto isso não é visto pela maioria, que ainda possui a ideia errônea de que a internet é um espaço sem lei.

A educação pública sobre os riscos e o reconhecimento de *deep fakes* é essencial para combater seu uso indevido. Pensando nisso a Comissão europeia fez a seguinte proposta⁴³:

⁴³ Almeida, Fernanda Campo. Deepfake: tecnologia permite colocar rosto e voz em outro corpo. Jul. 2020. Disponível em: <https://vejasp.abril.com.br/cultura-lazer/deepfake-tecnologia-permite-copiar-o-rostoe-expressao-e-a-voz/>. Acesso em: 15 ago. 2021. 95SIQUEIRA, Paulo Alexandre Rodrigues de. O 'Deep Fake' e a Legislação Brasileira - utilização de instrumentos legais para a proteção à imagem. Conteúdo Jurídico, Brasília-DF: 29 set 2021. Disponível em: <https://conteudojuridico.com.br/consulta/artigo/53256/o-deep-fake-e-a-legislao-brasileira-utilizao-deinstrumentos-legais-para-a-proteo-imagem>. Acesso em: 20 set. 2023.

- i) obter maior transparência na divulgação de notícias online, inclusive em relação a como os dados pessoais são usados para direcionar informações aos leitores;
- ii) promover competências em educação para a mídia ("media literacy"), a fim de auxiliar usuários a navegar num mundo com superabundância de informação;
- iii) desenvolver instrumentos e ferramentas para que jornalistas, aliados a cidadãos, possam combater a desinformação;
- iv) impulsionar a diversidade e a sustentabilidade dos meios de comunicação;
- v) estimular estudos continuados sobre o impacto da desordem informacional, tratando deles com análises científicas.

Tendo em vista o crescente uso da internet pela sociedade foi criado o Comitê Gestor de Internet (CGI) buscando estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil. O Comitê publicou em 2012 uma Cartilha de Segurança para Internet, o documento traz recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Este comitê tem como atribuições o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil; diretrizes para a administração do registro de nomes de domínio usando <.br> e de alocação de endereços Internet (IPs); promoção de estudos e padrões técnicos para a segurança das redes e serviços de Internet; trazer recomendações de procedimentos, normas e padrões técnicos operacionais para a internet no Brasil; e a promoção de programas de pesquisa e desenvolvimento relacionados à internet, incluindo indicadores e estatísticas, estimulando sua disseminação em todo território nacional. Ademais a Cartilha apresenta o significado de diversos termos e conceitos utilizados na Internet, bem como aborda os riscos de uso desta tecnologia (CGI, 2012, p.03).⁴⁴

⁴⁴ COMITÊ GESTOR DA INTERNET NO BRASIL. Cartilha de Segurança para Internet. Versão 4.0 / CERT.br. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 23 set. 2023.

6 CONCLUSÃO

Deep Fakes nada mais é do que a junção de *Deep Learning* com *Fake*, produzindo assim vídeos ou imagens falsas. Esta tecnologia representa um desafio significativo para os direitos da personalidade e o Direito Penal. Os impactos nos direitos à privacidade, à imagem e à reputação são evidentes, e as lacunas legais existentes precisam ser abordadas de maneira eficaz.

A adaptação do Direito Penal para lidar com os casos de *Deep Fake* é crucial para garantir a integridade do sistema de justiça e proteger os direitos fundamentais dos indivíduos. Isso requer uma legislação específica, bem como esforços contínuos de educação e conscientização. Ressalta-se que a *Deep Fake* fere o direito à privacidade, imagem e a reputação do indivíduo, por se tratar do uso indevido de uma imagem, voz ou vídeo de terceiro.

Em um mundo cada vez mais digital, é fundamental que a sociedade e o sistema legal estejam preparados para enfrentar os desafios apresentados pela tecnologia *Deep Fake* e garantir que os direitos da personalidade sejam preservados na era digital. Entretanto temos atualmente poucas legislações, como a Lei nº 12.965/2014 que não trata especificadamente da proteção de imagem, mas traz alguns benefícios indiretos que podem ser usados para proteger principalmente a imagem do indivíduo. Assim conclui-se que ainda falta uma proteção à privacidade da pessoa no âmbito digital, e isso só conseguira melhorar com leis específicas, assim como a responsabilidade dos provedores, onde vemos pessoas com a ideia de que a internet é uma terra sem lei, e que irá estar salva pelo anonimato. O Marco Civil da Internet foi o primeiro passo do Brasil para uma efetiva proteção do indivíduo, pois garante uma liberdade de expressão online e ao mesmo tempo consegue proteger a imagem da pessoa na era digital. Com um direito midiático, a proteção à imagem deve ser encarada dentro do seu tempo, mas com base no direito da personalidade, como atributo essencial da dignidade da pessoa humana.

Fato é que a tecnologia transforma a cada dia a forma de se capturar a imagem, mas permanece atual a advertência de que o norte de todo o esforço hermenêutico

deve ser garantir que o direito à imagem cumpra sua função primacial de assegurar à pessoa humana o livre desenvolvimento dos atributos de sua personalidade, que compõem a sua dignidade.

REFERÊNCIAS

ALMEIDA, F. C. **Deepfake: tecnologia permite colocar rosto e voz em outro corpo**. Jul. 2020. Disponível em: <https://vejasp.abril.com.br/cultura-lazer/deepfake-tecnologia-permite-copiar-o-rosto-expressao-e-a-voz/>. Acesso em: 15 ago. 2021.

ÁVILA, G. N.; CORAZZA, T. A. M. . A Hiperexposição pessoal e seus reflexos nos direitos da personalidade: necessidade de uma tutela transversal do direito à privacidade, com enfoque no âmbito penal. **Juris Poiesis**, v. 25, p. 144-177, 2022.

ÁVILA, G. N.; CORAZZA, T. A. M. **A hiperexposição pessoal e o direito ao esquecimento e à intimidade**. <http://dx.doi.org/10.26668/IndexLawJournals/2526-0200/2022.v8i1.8627>, v. 1, p. 22-42, 2022. Acesso em: 15 ago. 2021.

BARBOSA, F. M. Estudo, desenvolvimento e comparação de técnicas de detecção de Deepfake. **Monografia (Bacharelado em Ciência da Computação)**. Universidade Federal do Maranhão. São Luís, 2018.

BRASIL. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 set. 2023.

BRASIL. Lei Nº 2.848, de 7 de dezembro de 1940. Institui o **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 set. 2023.

BRASIL, D. R.; Bento, L. A. (2023). O direito fundamental à privacidade no contexto da Lei Geral de Proteção de Dados. **Revista De Direito Contemporâneo UNIDEP**, 1(2), 7–24. Recuperado de <https://periodicos.unidep.edu.br/rdc-u/article/view/162>. Acesso em: 20 Set. 2023.

FIDELIS, V. C. ; SOARES, D. V. Os desafios do ordenamento jurídico brasileiro frente às deepfakes. **Revista Pensamento Jurídico**, São Paulo, Brasil, v. 17, n. 1, 2023. Disponível em: <https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711> . Acesso em: 22 set. 2023

CRUZ, M. A. R. C. ; CAMARGO, L. H. K. O direito fundamental à proteção de dados pessoais e as condições de precedência em três medidas não farmacológicas adotadas pelo Brasil no enfrentamento da Covid-19. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 16, n. 1, e48479, jan./abr. 2021. ISSN 1981-3694. DOI: <http://dx.doi.org/10.5902/19813694>

48479. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/48479> Acesso em: 24 Set. 2023.

LIMA, R. **Deepfake: o que é e como funciona?** 2020. Disponível em: <https://www.tecmundo.com.br/internet/206706-deepfake-funciona.htm> Acesso em: 20 set. 2023.

LOPES, A. **'Deepfake', o novo e terrível patamar das 'fake news'**. Jan. 2021. Disponível em: <https://veja.abril.com.br/tecnologia/deepfake-o-novo-e-terrivel-patamar-das-fake-news> Acesso em: 18 set. 2023.

LUCENDO, G. A. **A longa história das notícias falsas.** Disponível em: https://brasil.elpais.com/brasil/2018/06/08/cultura/1528467298_389944.html. Acesso em: 19 set. 2023.

NUNES, D. J. C. ; ANDRADE, O. M. O uso da inteligência artificial explicável enquanto ferramenta para compreender decisões automatizadas: possível caminho para aumentar a legitimidade e confiabilidade dos modelos algorítmicos? **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 18, n. 1, e69329, 2023. ISSN 1981-3694. DOI: <http://dx.doi.org/10.5902/1981369469329>. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/69329> Acesso em: 25 Set. 2023.

ROSA, J. L. G. Fundamentos da Inteligência Artificial. Rio de Janeiro: LTC, 2011, p. 3.

SIQUEIRA, D. P. ; VIEIRA, A. L. S. F. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 17, n. 3, e67299, set./dez. 2022. ISSN 1981-3694. DOI: <http://dx.doi.org/10.5902/1981369467299>. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/67299> Acesso em: 25 Set. 2023.

TEFFÉ, C. A. S. Considerações sobre a proteção do direito à imagem na internet. **Revista de Informação Legislativa: RIL**, v. 54, n. 213, p. 173-198, jan./ mar. 2017. Disponível em: http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p173 . Acesso em: 25 Set. 2023.

Sobre a Autoria

1 – Giovanna Aleixo Gonçalves Oliveira

Mestranda em Ciências Jurídicas pela Universidade Cesumar

<https://orcid.org/0009-0003-8232-0373> • giovana.aleixo97@gmail.com

Contribuição: Escrita e primeira redação

2 – Gustavo Noronha de Ávila

Doutorado em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul.

<https://orcid.org/0000-0002-7239-1456> • gusnavila@gmail.com

Contribuição: Escrita e primeira redação

Como fazer referência ao artigo (abnt):

OLIVEIRA, G. A. G.; ÁVILA, G. N. Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 19, e85239, p. 1-19, 2024. Disponível em: <https://doi.org/10.5902/1981369485239> Acesso em: dia mês abreviado. ano.

Direitos autorais 2024 Revista Eletrônica do Curso de Direito da UFSM

Editores responsáveis: Rafael Santos de Oliveira, Angela Araujo da Silveira Espindola, Bruna Bastos.



Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.