CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES

D598
Direito penal e cibercrimes [Recurso eletrônico on-line] organização Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores Ana Carolina Juzo, Clóvis Volpe Filho e Stephani Dettmer Di Martin Viena – Franca: Faculdade de Direito de Franca, 2023.

Inclui bibliografia
ISBN: 978-65-5648-917-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios da Regulação do Ciberespaço.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2023 : Franca, SP).

CDU: 34

CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES

Apresentação

É com grande satisfação que apresentamos os Anais do Primeiro Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet, realizado entre os dias 12 e 15 de setembro de 2023, na Faculdade de Direito de Franca, composta por trabalhos apresentados nos Grupos de Trabalhos que ocorreram durante o evento, após rigorosa e disputada seleção.

Ditos trabalhos, que envolvem pesquisas realizadas nas mais diversas áreas do direito, mas primordialmente relacionados a temas centrados na relação entre o direito e o impacto das tecnologias, apresentam notável rigor técnico, sensibilidade e originalidade, buscando uma leitura atual e inovadora dos institutos próprios da área.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões que ocorreram no evento por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Coordenação do Evento:

Alexandre Veronese (UnB)

Felipe Chiarello de Souza Pinto (Mackenzie)

José Sérgio Saraiva (FDF)

Lislene Ledier Aylon (FDF)

Orides Mezzaroba (CONPEDI/UFSC)

Samyra Naspolini (FMU)

Sílzia Alves (UFG)

Yuri Nathan da Costa Lannes (FDF)

Zulmar Fachin (Faculdades Londrina)

Realização:

Faculdade de Direito de Franca (FDF)

Grupo de Pesquisa d Políticas Públicas e Internet (GPPI)

Correalização:

Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI)

Faculdades Londrina

Universidade Federal de Goiás (UFG)

Universidade Presbiteriana Mackenzie (UPM)

Mestrado Profissional em Direito da UFSC

A UTILIZAÇÃO DA TECNOLOGIA DO DEEP FAKE EM FRAUDES FINANCEIRAS: UMA ANÁLISE SOB A PERSPECTIVA DO CIBERCRIME

THE USE OF DEEP FAKE TECHNOLOGY IN FINANCIAL FRAUDS: AN ANALYSIS FROM THE PERSPECTIVE OF CYBERCRIME

Maria Eduarda Rocha Verissimo [1]
Yasmin Marcelino Lourenço [2]
Yuri Nathan da Costa Lannes [3]

Resumo

A atual evolução digital fez com que os delitos se adaptassem a nova realidade, onde os criminosos aproveitam da tecnologia para cometerem infrações como fraudes financeiras. O presente trabalho tem como iniciativa observar como a utilização do Deep Fake pode ocorrer em fraudes financeiras, ofendendo a privacidade e segurança de empresas, instituições financeiras e indivíduos. Através do método bibliográfico e hipotético-dedutivo, concluímos a que, dessa forma, a legislação combinada da prevenção é essencial para extinguir o acontecimento desses crimes, onde a conscientização e o uso de tecnologias de segurança são de grande apoio sob a égide da população.

Palavras-chave: Deep fake, Fraude financeira, Cibercrime

Abstract/Resumen/Résumé

The current digital evolution has made crimes adapt to the new reality, where criminals take advantage of technology to commit offenses such as financial fraud. The present piper has the initiative to observe how the use of Deep fake can occur in financial fraud, offending the privacy and security of companies, financial institutions and individuals. Through the bibliographic and hypothetical-deductive method, we conclude that, in this way, the combined legislation of prevention is essential to extinguish the occurrence of these crimes, where awareness and the use of security technologies are of great support under the aegis of the population.

Keywords/Palabras-claves/Mots-clés: Deep fake, Financial fraud, Cybercrime

---

[1] coautor

[2] coautor

[3] Orientador

1) Introdução (contendo Objetivos e Metodologia)

Com a evolução das tecnologias, consequentemente, notamos que o acesso a informações e com o advento de inteligência artificial cresce a preocupação da utilização nociva que podem gerar a manipulação de evidências inautênticas nas transações financeiras. No caso dessa presente pesquisa, os "*deep fakes*" utilizam da inteligência artificial (IA) para forjar fotos e vídeos com pessoas reais e/ou famosas para convencer os telespectadores de utilizar daqueles serviços.

A pesquisa visa problematizar a forma que criminosos conseguem utilizar as novas tecnologias de inteligências artificiais para praticar golpes financeiros, a ausência da segurança e privacidade entre as informações pessoais de usuários. Outrossim, busca-se responder, qual a perspectiva sobre a responsabilização penal e a de prevenção contra criminosos que utilizam da tecnologia *Deep Fake* para fraude de finanças?

Diante disso, o objetivo geral se caracteriza em analisar as medidas que os criminosos adotam na tentativa de aplicar golpes a partir da tecnologia do "*deep Fake*" e parâmetros de medidas proativas para proteger clientes, investidores e o sistema financeiro como um todo é crucial diante de "*deep fakes*" em fraudes financeiras.

Ao compreender esse fenômeno, destaca-se os objetivos específicos como as organizações financeiras e reguladores podem mitigar as consequências para as vítimas e desenvolver estratégias de prevenção e detecção. Isso não apenas protege a confiança e a integridade no mercado, mas também fortalece a segurança geral do setor financeiro.

Na elaboração desta pesquisa será necessário a utilização do método bibliográfico, com vasta exploração de materiais já publicados, como livro, revistas e artigos científicos. a partir disso, é crucial a implementação do método dedutivo, criando argumentos embasados dessas premissas

2) Desenvolvimento

2. INTELIGÊNCIA ARTIFICIAL E *DEEP FAKE*

Com o avanço da tecnologia, o uso da inteligência artificial (IA) visa expandir horizontes, ficando cada vez mais acessível aos usuários a partir do século XXI. Seu crescimento exponencial gerou aprimoramentos de suas funções graças a competição empresarial em busca de inovações e desenvolvimento. No entanto, notamos a dificuldade de

encontrar a autoria e materialidade em crimes cibernéticos. O *Deep Fake* como popularmente conhecido, é uma tecnologia que permite a produção de vídeos, gravações de áudio ou imagens falsas e convincentes utilizando de imagens já existentes de outras pessoas.

Apesar do nome original ser "fakevideo", aprimorado pela equipe de cientistas da computação da Universidade de Washington ("UW") que obtiveram resultados a partir de algoritmos, assim como as inteligências artificiais, possibilitaram a simulação um vídeo do ex-presidente Barack Obama com base de áudios e imagens existentes. O termo *deep fake* tornou-se comum no ano de 2017 quando um usuário da plataforma *Reddit* com o pseudônimo *Deep Fake*, por ser uma junção das palavras *deep learning* (aprendizado profundo) e *fake* (falso), utilizando dos programas de software na produção de troca de rosto de celebridades em vídeos pornográficos, o que chamou a atenção da mídia e o causou o impacto dessa tecnologia.

A utilização da manipulação dos algoritmos ganhou espaço nas últimas décadas, o *Deep Fake* assessora na reprodução de rostos a partir de inteligência artificial. Os criminosos usufruem e fraudam a partir de redes neurais e artificiais conectadas em dubles que posteriormente será substituído pela imagem da pessoa, no entanto, só é possível ser feito com banco de dados alimentados por imagens da pessoa em questão.

Todavia, para a mídia ficar cada vez mais realista é necessário utilizar mais de uma inteligência artificial, no vídeo, é necessária uma simulação de áudio conhecido como *Deep Dub*, feitos com interação, uma gerando o conteúdo e a outra analisando as operações de confundir as fusões de imagens com a realidade.

2.1 *DEEP DUB* E SIMULAÇÃO DE ÁUDIO

A inteligência artificial utilizada na dissimulação dos algoritmos do *Deep Fake* é capaz de capitalizar e padronizar *log* com maior facilidade em fatos não factíveis aos humanos. A uniformização dos códigos também ajuda na detecção de anomalias e prevenção de manutenção.

Por entender esses padrões, a primeira coisa que começou a evoluir foram os sensores de som, movimentação e imagens, devido a expansão da tecnologia e a ascensão da internet das coisas (IoT), já que constantemente estamos reunindo, transmitindo e alimentando o banco de dados da internet promovendo a evolução da inteligência artificial.

Utilizando o mesmo sistema de algoritmo do *Deep Fake*, o *Deep Dub* é capaz de realizar uma simulação de voz e áudios, ficando cada vez mais autêntico e de difícil

identificação da realidade. Essa simulação digital de som é de fácil acesso, muito sites permitem essa funcionalidade com algumas restrições.

2.2 REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL

A evolução dos programas de software a parir da linguagem de programação, sistema operacionais, banco de dados (relacionais), processadores de textos, interface gráfica, sistemas clientes-servidor, computação em nuvem grande trouxeram mudança, com isso grandes impactos na tecnologia. A Inteligência artificial (IA) não pode ser considerada uma evolução de software, mas um novo começo na criação de novos programas de software. Em setembro de 2021 foi aprovada o projeto de lei nº 21/2020 que criou o marco legal do desenvolvimento da inteligência artificial, destacando a relevância da inovação para o crescimento econômico e desenvolvimento humano e social.

Não obstante dos *Deep Fakes* não ter lei especifica que regulamente sobre o uso no Brasil, praticas fraudulentas, incluindo roubo de identidade, falsificação, golpes financeiros e outras práticas enganosas que visam obter ganhos financeiros de maneira ilegal são crimes previstos no nosso atual Código Penal (Decreto-Lei nº 2.848/1940), em seu artigo artigo 171 prevê a pratica de estelionato quando tem a intenção de tirar vantagem alheia de forma ilícita levando a pessoa a erro ou acarretando ao prejuízo e, geralmente, esses crimes são pensados ardilosamente e organizadamente em Formação de Quadrilha ou Bando aplicando o artigo 288 do mesmo Código. Há também legislação extravagantes, como a Lei nº 7.492/1986 (Crime Contra o Sistema Financeiro Nacional), dispõe sobre fraudes emissão irregular de títulos de crédito e manipulação de mercado, no entanto por ser tratar por crimes que aproveitam da inteligência artificial emprega a Lei nº 12.737/2012 (Lei Carolina Dieckmann) contra Crimes Cibernéticos.

2.2 FRAUDES FINANCEIRAS

Na era digital, a maior parte das transações são realizadas *online*, tornando-as cada vez mais rápidas e descomplicadas, permitindo que sejam feitas sem sair de casa. No entanto, a tecnologia acessível também oferece oportunidades para criminosos cometerem delitos como a fraude financeira, como meio de uma das ferramentas a serem usadas, o *Deep Fake*. O uso dessa Inteligência Artificial não se enquadra como crime, mas, a utilização dela com malícia, é ilegal e possível de ser tipificada.

A fraude financeira no espaço cibernético é um crime que afeta cada vez mais empresas, instituições financeiras e indivíduos, podendo causar sérios prejuízos ao bem jurídico

alheio. A tendencia é que essa espécie de crime se torne cada vez mais comum com a acessibilidade da tecnologia para todos.

No primeiro semestre de 2021, houve um aumento no número de tentativas de fraude em compras digitais. Um levantamento da empresa antifraude Clearsale monitorou mais de 152 milhões de transações digitais nos primeiros seis meses deste ano, das quais 2,6 milhões foram tentativas de roubo por parte de golpistas. Comparado ao mesmo período de 2020, houve um aumento de 32,7% nas tentativas de fraude.

O *Deep Fake* permite uma pessoa se passar por outra, sendo capaz de burlar sistemas de validação de identidade. Para praticar as fraudes com essa ferramenta, os criminosos podem criar várias modalidades de golpes.

Na "Fraude fantasma", os criminosos utilizam os dados de pessoas falecidas para obter benefícios, como solicitar cartões de crédito ou obter empréstimos em bancos.

Por sua vez, ocorre com a "Fraude de conta nova" um crime onde o fraudador adota uma identidade roubada para cometer esses crimes, utilizando o *phishing***,** uma forma de roubar dados do indivíduo onde a vítima é induzida a clicar em um link que se passa por uma empresa confiável, sendo revelado suas informações pessoais. Dessa forma, os criminosos utilizam o *Deep Fake* se passando por uma pessoa real e conseguem criar a conta. Na maioria dos casos, o fraudador cria várias contas e utiliza o cartão de crédito para realizar compras online.

Já na "Fraude de identidade sintética", o criminoso combina dados de diferentes pessoas, criando uma nova identidade que é mais complexa de detectar. Por meio disso, o infrator realiza grandes transações e solicitações de crédito usando os dados de várias pessoas.

O anonimato da internet favoreceu o crescimento desses tipos de crimes, podendo ocorrer a "fuga perfeita", onde há complicações na hora de encontrar a autoria e materialidade do criminoso e, consequentemente, levá-lo a julgamento. Apesar de parecer desafiador, as empresas e indivíduos devem lutar contra isso e estarem atentando a sinais de fraude, reconhecendo suas formas e analisando suas ações.

2.2.1 LEGISLAÇÃO

A realidade do tempo de criação do Código Penal, em 1940, era bem diferente de atualmente, onde diversas tecnologias foram criadas, mudando muitos aspectos em nossas vidas, sendo um deles as transições financeiras.

Para se adequar com o momento em que estamos vivendo, onde os crimes também podem ocorrer na esfera cibernética, o CP, em seu Art. 171, que discorre sobre o estelionato,

crime caracterizado pela vontade de um sujeito de obter vantagem própria através de artimanha, induzindo ou mantendo um indivíduo em erro por meio de artifício, em maio de 2021, incluiu o art. 154-A, e os parágrafos 2º-A e 2º-B, mostrando a possibilidade do crime nos ambientes virtuais. A pena para quem comete este tipo de delito é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa. De acordo com a doutrina, o estelionato é um delito que apresenta dupla consequência, onde, de um lado, há a obtenção de uma vantagem ilícita e, por outro lado, a efetiva ocorrência de prejuízo para a vítima. Geralmente, esses resultados ocorrem simultaneamente, mas é possível que um deles se concretize e o outro não. Nessa situação, o crime não será consumado. (GONÇALVES, 2012, p 184).

É fato que a lei seja de suma importância para combater o crime, mas, além dela, a prevenção é essencial. Propagando a conscientização, que funciona com a educação digital, onde o acesso à informação é necessário para advertir os riscos de golpe que existem na internet, também é valido a tomada de medidas de segurança, onde se deve evitar passar seus dados pessoais em locais suspeitos, não clicar em links desconhecidos e fazer a monitoração de suas transações financeiras. Para as empresas, o uso de sistemas de segurança avançadas e detectores de fraude são a melhor opção.

Logo, o combate contra a fraude financeira digital tem duas faces. Além da necessidade de uma legislação sobre o assunto, também é preciso da prevenção. Para se defender, a educação digital é essencial, pois, entendendo o *modus operandi* do crime e suas modalidades, menos ocorrências teremos.

3) Conclusão

Em consonância com a vida moderna o aumento do uso da tecnologia do *Deep Fake* para ações maliciosas, sem o consentimento das pessoas deixou essa tecnologista malvista aos olhos de todo mundo, sendo ligada até mesmo em notícias de desinformações e *Fake News*. Apesar de ser usada a fim de entretenimento e prestações de serviços. Nesse sentido, denota-se a importância da presente pesquisa e atuais desafios para instituições financeiras.

Todavia, sobre a perspectiva de responsabilização penal do indivíduo é incerto, já que autoria e materialidade do crime, por uma vez, o crime consiste na falsificação da própria identidade, prejudicando na persecução penal e seu armazenamento na cadeia de custódia, principalmente na valoração e admissibilidade das provas digitais com a ausência de autenticidade das evidências. Apesar de não possuir legislação própria, analogicamente, leis existentes podem se enquadrar na tipificação de crimes ocorridos por meio de *Deep Fake*.

Por se tratar de instituições financeiras é necessária uma intervenção ação de cooperação internacional e ajuda de novas tecnologias que permitem, como prevenção, a partir de uma rede neural gerar milhares de imagens, dependendo do sistema em uso, adotando um mecanismo capaz de decifrar a sequência e padronização lógica por traz dos algoritmos presentes na programação de *Deep Fake*, dessa forma essa nova inteligência artificial com potencial e competência de apontar a autenticidade de imagens ou vídeos gerados.

4) Referências

CHARGEBACKS911. **Ocorrência de Fraude em Novas Contas: Entendendo o Novo Tipo de Fraude com Cartões de Crédito e Débito.** Chargebacks911, 20 set. 2023. Disponível em: https://chargebacks911.com/new-account-fraud/#:~:text=New%20account%20fraud%20occurs%20when,new%20credit%20or%20debit%20cards. Acesso em: 26 jul. 2023.

CLEARSALE. **Mapa da Fraude: Tendências e Estatísticas de Fraude Online.** ClearSale, 15 jul. 2023. Disponível em: https://br.clear.sale/mapa-da-fraude. Acesso em: 26 jul. 2023

FORBES TECH. **Quais os limites éticos e legais no uso de deepfake?** Forbes, 25 jul. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/07/quais-os-limites-eticos-e-legais-no-uso-de-deepfake/. Acesso em: 26 jul. 2023.

GONÇALVES, V.E.R. Dos Crimes Contra o Patrimônio. Vol. 9. 15º Ed. São Paulo: Saraiva, 2012

MEDON AFFONSO, F. J. **O direito à imagem na era das deep fakes**. Revista Brasileira de Direito Civil, [S. l.], v. 27, n. 01, p. 251, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438. Acesso em: 23 jul. 2023.

RIBEIRO, E. S. **Crime de estelionato – uma análise da evolução sob a égide da impunidade na cidade de Manaus**. Artigo nda Revista Cientifica - Semana Acadêmica: 2019, disponível em: https://semanaacademica.org.br/search/node/Eliete%20da%20Silva%20Ribeiro

Robert Chesney & Danielle Keats Citron, Deep Fakes: **Um desafio iminente para privacidade, democracia e segurança nacional**, 107 CAL. L. REV. 1753, 1760 (2019) (notas de rodapéomitidas); Jennifer Langston, Lip-Syncing Obama: Novas ferramentas transformam clipes de áudio em vídeos realistas, UW NEWS (11 de julho de 2017), https://www.washington.edu/news/2017/07/11/lipsyncing-obama-new -tools-turn-audio-clips-into-realistic-video/