II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

RESPONSABILIDADE CIVIL E TECNOLOGIA

R434
Responsabilidade civil e tecnologia [Recurso eletrônico on-line] organização II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Liton Lanes Pilau Sobrinho, Alisson Jose Maia Melo e Marcelo Toffano – Franca: Faculdade de Direito de Franca, 2024.

Inclui bibliografia
ISBN: 978-65-5274-014-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Regulação do Ciberespaço.
1. Responsabilidade Civil. 2. Tecnologia. 3. Relações de Consumo. 4. Políticas Públicas de Desenvolvimento. 5. Efetividade do Direito. I. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2024 : Franca, SP).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

RESPONSABILIDADE CIVIL E TECNOLOGIA

Apresentação

Entre os dias 27 e 30 de agosto de 2024, a Faculdade de Direito de Franca recebeu o Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 10 – Responsabilidade Civil e Tecnologia dedicou-se ao estudo das interfaces entre responsabilidade civil e tecnologia, abordando os princípios que orientam a responsabilidade civil no contexto contemporâneo. Foram discutidos temas como a responsabilidade subjetiva e objetiva, tanto em contratos quanto fora deles, e a responsabilidade das pessoas jurídicas e de seus administradores em um ambiente cada vez mais influenciado por tecnologias. As discussões também se aprofundaram na responsabilidade por fato de outrem e nas implicações tecnológicas nas relações de consumo, enfatizando como as novas tecnologias desafiam e reconfiguram os conceitos tradicionais da responsabilidade civil. Este GT trouxe reflexões essenciais sobre a adaptação dos marcos jurídicos para responder às exigências de uma sociedade digital e conectada.

ALGORITMOS ENGANOSOS: O TRÁFEGO DE PUBLICAÇÕES QUE UTILIZAM DEEPFAKE NAS REDES SOCIAIS PARA ENGANAR OS USUÁRIOS OU PRATICAR CRIMES

DECEPTIVE ALGORITHMS: THE TRAFFIC OF PUBLICATIONS THEY USE DEEPFAKE ON SOCIAL MEDIA TO DECEIVE USERS OR COMMIT CRIMES

Lucas Gabriel Alecrim [1]

Resumo

O presente resumo expandido contempla as pesquisas preliminares feitas sobre a temática da existência de responsabilidade civil das redes sociais quando o conteúdo malicioso é patrocinado pela própria plataforma, bem como analisar essas publicações maliciosas, em especial as que usam a tecnologia DeepFake para ludibriar o usuário, com o intuito de desenvolver formas de como as plataformas de redes sociais podem valer-se de seus próprios algoritmos internos para que, em vês de contribuir para a divulgação destas publicações falsas, ajudem a combatê-las.

Palavras-chave: Deepfake, Regulação das redes sociais, Golpes digitais, Internet

Abstract/Resumen/Résumé

This expanded summary includes preliminary research on the subject of the existence of civil liability of social networks when malicious content is sponsored by the platform itself, as well as analyzing these malicious publications, especially those that use DeepFake technology to deceive the user, in order to develop ways in which social media platforms can use their own internal algorithms so that, instead of contributing to spread these false publications, help to combat them.

Keywords/Palabras-claves/Mots-clés: Deepfake, Social media regulation, Digital scams, Internet

[1] Estudante de Graduação na Faculdade de Direito de Franca e Pesquisador do Programa de Iniciação Científica da Faculdade de Direito de Franca de 2023 a 2025.

1 INTRODUÇÃO

Durante a última década o mundo experenciou uma grande evolução nas comunicações socias e no desenvolvimento de Inteligências Artificiais (I.A) que utilizam o chamado deep learning, uma tecnologia de aprendizagem de máquina que permite que o programa aprenda como um cérebro humano pois é desenvolvido nos moldes de redes neurais. Tal evolução possibilitou que surgissem as I.As Generativas, programas que utilizam conceitos de I.A tradicionais adicionados a tecnologia deep learning, e desta forma conseguem gerar imagens, vídeos e até áudios a partir de comandos simples, e tinham a promessa de revolucionar inúmeras áreas da vida humana, desde a medicina até a indústria, da economia à arte.

No entanto esse tipo de programa começou a ser usado de formas que passou e ser relevante para o Direito e uma dessas formas ficou conhecido como Deepfake, a palavra tem origem na junção das palavras “deep learning” e “fake” e consiste, em linhas gerais, em uma técnica de manipulação de mídia que usa a Inteligência Artificial para criar conteúdo audiovisual falso, geralmente envolvendo a substituição do rosto de uma pessoa em um vídeo por outro rosto, e a utilização mais perigosa é quando o vídeo é verdadeiro mas o conteúdo da fala é adulterado, em outras palavras, uma pessoa pode ter um vídeo seu realista dizendo coisas que nunca disse.

Entretanto, a situação se agrava quando esses vídeos falsos são publicados nas redes sociais e disseminam conteúdos enganosos aos usuários de forma que podem levar um grande número de pessoas a acreditarem que determinada pessoa fez ou disse algo que não é real, ademais algumas dessas publicações falsas são publicadas como conteúdo de tráfego pago disseminadas pelos próprios algoritmos das redes socias a mais e mais pessoas.

Deste modo, o objeto de pesquisa deste trabalho é realizar um estudo sobre a disseminação de deepfakes pelas redes sociais, no entanto dada a extensão do tema uma delimitação é necessária fazendo com que o pesquisado neste trabalho seja como os algoritmos das redes sociais lidam com publicações que utilizam o deepfake para enganar os usuários e eventualmente para praticar crimes, como violação de imagem pessoal e até mesmo estelionato, e após isso ponderar sobre uma eventual responsabilidade civil pelos danos causados a pessoas vítimas dessas publicações, em especial se forem publicações de tráfego pago. Salienta-se ainda que serão analisados apenas as redes socias Instagram, Facebook e TikTok.

A problemática central que a pesquisa buscará resolver é: qual é o grau de participação e consequente responsabilização das redes sociais na divulgação de postagem que contenham

deepfakes que visam enganar ou aplicar golpes aos outros usuários? E como o uso de deepfakes nas redes socais impactam o mundo jurídico?

Para responder os problema de pesquisa será utilizado o método hipotético-dedutivo, esse trabalho também se valerá da pesquisa bibliográfica feita a partir do levantamento de artigos publicados por meios impressos ou eletrônicos e páginas de web sites com referencial teórico pertinentes a temática da pesquisa, bem como será realizada uma pesquisa documental em fontes diversas buscando uma mais vasta base de informações oficiais relevantes tais como tabelas estatísticas e infográficos sobre a temática dos algoritmos e deepfakes nas redes sociais.

A pesquisa contará como referencial teórico Manuais de Direito Digital e livros específicos sobre a Regulação das Plataformas de relevantes expoentes do mundo jurídico sobre o tema como: Tatiana Stroppa, Sarah Littman, Américo Ribeiro Magro e Landolfo Andrade.

2 DESENVOLVIMENTO

2.1 Conceito de DeepFake

O Dicionário *Cambridge* define *Deepfake* como "uma gravação de áudio ou vídeo que substitui o rosto ou a voz de alguém pela de outra pessoa, de uma forma que pareça real". Desta forma, quando, na realidade atual, existem uma grande disponibilidade de ferramentas on-line capazes de facilmente criar manipulações de conteúdo, os autores Paris e Donovan (2019) chamam os *Deepfakes* elaborados por meio de programas de computador disponíveis gratuitamente e que normalmente tem menos qualidade do que os que são elaborados por softwares mais complexos de *cheap fake*, assim:

> Outras formas de manipulação audiovisual – *"cheap fakes"* – dependem de software barato e acessível, ou de nenhum software. Ambos deepfakes e *cheap fakes* são capazes de borrar a linha entre expressão e evidência. Ambos podem ser usados para influenciar a política das evidências: como as evidências mudam e são alteradas por sua existência em estruturas culturais, sociais e políticas. (PARIS; DONO-VAN, 2019, p. 2–3)

Portanto as manipulações tanto de *Deepfakes* mais complexos quanto dos chamados *cheap fakes* podem causar efeitos danosos na sociedade e principalmente nas redes sociais, onde são usados atualmente de uma forma mais complexa para ludibriar o usuário e induzi-lo a cair em golpes minuciosamente elaborados.

2.2 As mídias sociais e os golpistas digitais

Na atualidade as redes sociais tais quais, Instagram, TikTok e Facebook, passam por uma onda de anúncios que são, em sua maioria, *deepfakes* de pessoas famosas anunciando uma loja ou aplicativo que está com desconto ou sendo uma oportunidade de ganhar dinheiro rápido e fácil. Para ilustrar isso Ludgero (2020) estimava que o Instagram poderia ter até 95 milhões de perfis falsos, a isso o autor complementa:

> O ambiente online acaba facilitando ações ilegais, por conta da dificuldade de rastrear o criminoso e a falta de informação dos internautas de como denunciar. Esses perfis são mais difíceis de identificar que do um fake comum, pois eles agem como se fossem reais — postam fotos, legendas, stories e informações que conferem legitimidade para o perfil, que pode ser pessoal ou institucional. (LUDGERO, 2020 p.1)

Desta forma, percebe-se que com o aumento dos potenciais criminosos as empresas detentoras de plataformas sociais deveriam efetuar adequações legais para suprimir as lacunas deixadas em seus termos de uso sobre os casos desses golpes digitais.

Dentre os golpes digitais os que tem a maior influencia dos *deepfakes* são os chamados "*money flipping*", modalidade em que o golpista oferece a oportunidade de dinheiro fácil ao usuário desatento, que muitas vezes tem que depositar uma pequena contia para ter a chance de ganhar o prêmio. Nos últimos meses o famigerado "Jogo do tigrinho" tem tomado conta dos vídeos de Instagram com a finalidade para atrair mais "clientes".

2.3 Da responsabilidade das plataformas

Nos casos de fraudes cometidas por usuários que tem como objetivo enganar os outros usurários das plataformas digitais o artigo 19 da Lei nº 12.965/ 2014 (Marco Civil da Internet) é claro no sentido da não responsabilização dos provedores de aplicação, nestes termos:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014, Art.19)

Deste modo, a questão da responsabilização em casos que o usurário é vítima de uma fraude que envolveu um conteúdo que foi patrocinado pela rede social é um tema controverso e que precisa ser discutido no âmbito jurídico pois com o aumento de casos de fraudes que se utilizam das redes socias para atingir o maior número de vítimas possível deve tomar atitudes para garantir tanto a liberdade do usuário na plataforma quanto os direitos do consumidor, que segundo Sérgio Cavalieri Filho (2019), não poderia assumir os riscos das relações de consumo, nem arcar com os prejuízos decorrentes dos acidentes de consumo sem indenização.

3 Resultados preliminares

O estudo ainda está em fase inicial de elaboração, e ainda há muita pesquisa para ser realizada, mas pode-se concluir preliminarmente que a internet deve ser palco para muitas discussões jurídicas sobre responsabilização das plataformas digitais sobre o conteúdo por elas patrocinado e discussões sobre como a Inteligência Artificial e os Algoritmos dessas mídias sociais são usados como impulsionadores do uso da tecnologia DeepFake para a aplicação de golpes que exploram “brechas” nos termos de uso das plataformas e enganam o usuário para obter ganhos financeiros ilícitos.

Ademais cita-se a necessidade de um estudo sobre as leis que se aplicam ao tema nos casos analisados bem como uma análise da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) verificando a possibilidade de responsabilização Civil e criminal dos envolvidos.

REFERÊNCIAS PRELIMINARES

BRUNDAGE, Miles et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. **ArXiv**, [S.l.], p. 1-101, 20 fev. 2018. Disponível em: https://doi.org/10.48550/arXiv.1802.07228. Acesso em: 18 abr. 2024.

CADETE FIDELIS, Vanderson; VERBICARO SOARES, Douglas. Os desafios do ordenamento jurídico brasileiro frente às deepfakes. **Revista Pensamento Jurídico**, v. 17, n. 1, 2023. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711. Acesso em: 27 abr. 2024.

CAVALIERI FILHO, Sergio**. Programa de responsabilidade civil**. 13 ed. São Paulo: Atlas, 2019.

FERRARA, Emilio. GenAI against humanity: nefarious applications of generative artificial intelligence and large language models. **Journal Of Computational Social Science**, [S.L.], p. 1-21, 22 fev. 2024. Disponível em: https://link.springer.com/article/10.1007/s42001-024-00250-1. Acesso em: 18 abr. 2024.

LITTMAN, Sarah Darer. **Deepfake**. 1. ed. New York: Scholastic Press, 2020.

LUDGERO, Paulo Ricardo. O que são Scammers? Entenda a fraude. **JusBrasil**, [S. l.], 2020. Disponível em: https://ludgeroadvocacia.jusbrasil.com.br/artigos/883306590/o-que-sao-scammers-entenda-a-fraude Acesso em: 27 jun. 2024.

MAGRO, Américo Ribeiro; ANDRADE, Landolfo. **Manual de Direito Digital**. 4. ed. rev. atual. e aum. São Paulo: Editora JusPodivm, 2024

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: 18 abr. 2024

PARIS, Britt; DONOVAN, Joan. *Deepfakes and cheap fakes*. **Thousand Oaks**: Sage (=Data & Society's Media Manipulation research initiative). Disponível em: https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf. 2019. Acesso em: 27 jun. 2024

PRADO, Magaly Parreira do. Deepfake de áudio: manipulação simula voz real para retratar alguém dizendo algo que não disse. **TECCOGS**: Revista Digital de Tecnologias Cognitivas, [S.L.], n. 23, p. 45-68, 12 out. 2021. Pontifical Catholic University of Sao Paulo (PUC-SP). Disponível em: https://revistas.pucsp.br/teccogs/article/view/55977. Acesso em: 18 abr. 2024

SANTAELLA, Lúcia; DE MATTOS SALGADO, Marcelo. Deepfake e as consequências sociais da mecanização da desconfiança. **TECCOGS**: Revista Digital de Tecnologias Cognitivas, [S.L.], n. 23, p. 90-103, 12 out. 2021. Pontifical Catholic University of Sao Paulo (PUC-SP). Disponível em: https://revistas.pucsp.br/index.php/teccogs/article/view/55981/37929. Acesso em: 27 jun. 2024

STROPPA, Tatiana. **Plataformas Digitais e moderação de conteúdos**: por uma regulação democrática. Belo Horizonte: Forum, 2021.