Deepfake: Implications and Solutions in the EU

AYSEGUL ZENGIN[1]

Abstract: *Deepfakes are hyper-realistic videos that apply artificial intelligence to depict persons' images and voices. Deepfake came into our lives when a Reddit moderator began posting videos that used face-swapping technology to insert celebrities' likenesses into existing pornographic videos in 2017. Despite a long time having passed, there is still no legal and technical solution in the European Union(the EU) to prevent creating or viraling of deepfake videos.*

This paper addresses the pressing need for effective measures to combat deepfake proliferation, acknowledging the inadequacy of existing legal and technical frameworks in the EU. Due to its technical aspects, privacy rights, intellectual rights, and criminal law are not good enough to protect the rights of persons' whose image or voice is used in deepfake videos. By undertaking a thorough examination, this study seeks to bridge the gap between the current state of technology and the legal safeguards required to protect individuals from the detrimental effects of deepfakes in the EU.
Keywords: *Deepfake, defamation, privacy, pornography, EU.*

INTRODUCTION

Deepfakes originated in 2017. An influential Reddit user utilized open-source software from Google and other platforms to leverage scattered academic research on face-swapping. This mentioned individual uploaded the manipulated clips that featured the faces of celebrities like Scarlett Johansson, Gal Gadot, and Taylor Swift superimposed onto the bodies of adult film actresses, marking an early and controversial use of deepfake technology.[2]

In 2018, a viral trend emerged on the internet involving the manipulation of videos featuring Nicholas Cage's face inserted into scenes from various Hollywood films, achieved through the use of deepfake technology. Despite the initial appearance of genuine performances, none of the showcased scenes originally involved Cage. The rise of deepfakes, powered by artificial intelligence, allowed users to seamlessly replace original actors' faces in videos. Nicholas Cage's prominent role in these manipulated videos, given his history in the film "Face/Off," where characters swap faces, added a notable dimension to the phenomenon.[3]

In another example, a deepfake video featuring Barack Obama surfaced online, depicting him referring to the then US President Donald Trump as a 'complete dipshit.' Another deepfake video emerged, showcasing Mark Zuckerberg falsely asserting 'complete control over people's data.[4] And, finally, in October 2023, actor Tom Hanks warned fans not to fall for deepfake advert using his face and added ''I have nothing to do''[5].

All these examples and also pornographic videos which are mostly used with deepfakes show how deepfake could be creative and disruptive. Because of the technology behind it, deepfakes remains unsolved and lack of specific regulations makes it harder to solve the problem. This article explains deepfakes in a comprehensive review, examines the current legal implications, and casts about for a solution in legal and technical ways in the EU.

[1] Project Assistant, Department of Law, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia, Email: azengi@taltech.ee

[2]Catherine Kerner & Mathias Risse, "Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds," in Moral Philosophy and Politics, VIII, No.2, 2020, p. 84

[3]Erik Gerstner, "Face/off: 'deepfake' face swaps and privacy laws," in Defense Counsel Journal, LXXXVII, No. 1, 2020, p. 1

[4]Madhura Thombre, "Deconstructing Deepfake: Tracking Legal Implications and Challenges," in International Journal of Law Management & Humanities, IV, 2021, p. 2269

[5]Seehttps://news.sky.com/story/tom-hanks-warns-fans-not-to-fall-for-deepfake-advert-using-his-face-12974902 Accessed 13.03.2024

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-997-9

1. WHAT IS DEEPFAKE?

Before deepfake, it is useful to define what synthetic media which consists deepfake as a subbranch in its family. Content categorized as synthetic media is wholly or partially crafted or altered through the application of AI or other technological methods. Deepfakes are the most advanced and realistic form of synthetic media. [6]

Deepfakes, a fusion of "deep learning" and "fake," are highly realistic videos digitally manipulated to portray individuals engaging in actions or utterances that never occurred in reality. This manipulation relies on neural networks, utilizing extensive data samples to emulate a person's facial expressions, gestures, voice, and tonal nuances. The process entails training a deep learning algorithm by inputting footage of two individuals, enabling it to interchange their faces seamlessly. In essence, deepfakes employ facial mapping technology and AI to substitute the face of one person in a video with that of another individual.[7]

The technology behind deepfake, rooted in deep learning, operates by analyzing extensive datasets of real recordings or images to learn and replicate the facial and vocal characteristics of a person. This adaptable model is then digitally imposed over another person's face seamlessly, resembling a mask. Early versions of deepfakes invoked an uncanny valley effect, generating somewhat human-like but clearly artificial outputs. However, the advent of generative adversarial networks (GANs) has significantly enhanced the sophistication and believability of deepfake outputs. GANs employ two neural networks, a generator and a discriminator, in an adversarial relationship, with the generator creating fake images and the discriminator learning to distinguish between authentic and computer-generated images. Through a continuous feedback loop, both networks improve, resulting in the generator producing highly realistic images that increasingly challenge detection by the discriminator. This reciprocal refinement process allows deepfake generators to create convincing content that closely resembles genuine images and recordings.[8]

2. BENEFITS OF DEEPFAKE

Even though there are negative examples and concerns about it, deepfake technology has numerous benefits. As like all technologies can be used for the advancement of science and society. For instance, the online gaming industry is exploring the use of deepfake technology, specifically 'artificial intelligence-generated voice skins,' to elevate the gaming experience for players. Through the incorporation of face cloning and voice cloning, the entertainment and advertising sectors can harness the full potential of this technology.[9]

Also, deepfake technology extends its utility to automatic and authentic voice dubbing for movies in various languages, enhancing accessibility for diverse audiences in enjoying films and educational content. Illustrated by a 2019 Malaria awareness campaign featuring David Beckham, deepfake applications successfully transcended language barriers through visual and voice-altering technology, presenting the celebrity as multilingual. Furthermore, in video conference calls, deepfake technology proves valuable by translating speech, synchronously adjusting facial expressions and mouth movements, thereby breaking down language barriers and fostering

[6] Bart van der Sloot & Yvette Wagensveld, "Deepfakes: Regulatory challenges for the synthetic society," in Computer Law & Security Review, XLVI, 2022, p. 4

[7] Mika Westerlund, ''The Emergence of Deepfake Technology: A Review'', in Technology Innovation Management Review, IX, No.11, 2019, p. 40

[8] Lindsey Joost, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in University of Florida Journal of Law and Public Policy, XXXIII, No.2, 2023, p. 314

[9] Madhura Thombre, "Deconstructing Deepfake: Tracking Legal Implications and Challenges," in International Journal of Law Management & Humanities, IV, 2021, p. 2269

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-762-3

improved communication where participants appear to be speaking the same language, enhancing eye-contact and overall engagement.[10]

Deepfake can serve as a tool for individuals coping with the loss of loved ones by digitally resurrecting a deceased friend, providing an opportunity for grieving loved ones to say their goodbyes. Moreover, deepfakes can digitally recreate limbs for amputees, assist transgender individuals in visualizing themselves as their preferred gender, and facilitate interactions for individuals with Alzheimer's by presenting familiar faces. Scientists are exploring the technology's potential in medical fields, including the detection of abnormalities in X-rays and the creation of virtual chemical molecules for accelerated materials science and medical discoveries. Lastly, in the business realm, deepfakes have caught the attention of brands, enabling transformative applications in e-commerce and advertising.[11]

3. THREATS OF DEEPFAKE

The prevalence of deepfake content is prominently skewed towards pornography, with a 2019 study revealing that 96% of the 14,678 deepfake videos on the internet were of a sexual nature. While initially featuring celebrities, the disturbing trend extends to ordinary individuals, turning deepfake pornography into a new form of non-consensual exploitation comparable to revenge pornography. Unlike traditional revenge porn, deepfake pornography allows perpetrators to create explicit videos using publicly available images, making virtually anyone susceptible to being victimized. Actress Scarlett Johansson highlighted the distressing reality, emphasizing the lack of control over one's image being manipulated and inserted into explicit scenarios, with potential severe consequences for victims.[12]

Another pervasive use of deepfake technology has the potential to sow widespread confusion and undermine the value of truth in today's world. The mere suspicion of deepfake manipulation can trigger chaos, leading to a significant erosion of trust in genuine content.

Moreover, even if the subjects immediately denounce the falseness of the content, the public may still be misled. The act of retracting the fake video often proves insufficient in countering the spread of misinformation. People's inclination to act on false information before retractions, as well as their tendency to reject evidence if it contradicts their preexisting beliefs, contributes to the persistence of misinformation.[13]

As deepfake content becomes increasingly prevalent, there is a heightened risk of discrediting authentic material as fake, contributing to what is termed 'the liar's dividend.' This phenomenon entails a pervasive suspicion surrounding all forms of media, creating a substantial trust deficit between public institutions and the general populace.[14]

Another potential threat of deepfake that offers criminals new avenues for deceiving individuals and organizations. Instances of fraud involve a CEO being duped into transferring $243,000 to a fraudster who used deepfake technology to replicate the boss's voice. Celebrities and public figures face misappropriation of their images for unauthorized advertising, such as Elon Musk impersonators promoting Bitcoin scams on Twitter and synthetic media images of BBC presenter

[10] Mika Westerlund, ''The Emergence of Deepfake Technology: A Review'', in Technology Innovation Management Review, IX, No.11, 2019, p. 41
[11] Ibid.
[12] Lindsey Joost, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in University of Florida Journal of Law and Public Policy, XXXIII, No.2, 2023, p. 317
[13] Nina I.Brown, ''Deepfakes and the weaponization of disinformation'', in Virginia Journal of Law & Technology, XXIII, No.1, 2020, p. 10
[14] Madhura Thombre, "Deconstructing Deepfake: Tracking Legal Implications and Challenges," in International Journal of Law Management & Humanities, IV, 2021, p. 2273

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-997-9

Carol Kirkwood being used to endorse diet pills without her knowledge. Martin Lewis, founder of MoneySavingExpert, took legal action against Facebook for allowing thousands of fake advertisements using his name and photo to circulate on the platform, citing defamation. These deceptive practices, leveraging the trust in well-known personalities, are poised to escalate with the advancement of deepfake and synthetic media technologies.[15]

Lastly, deepfake technology has extended into courtrooms. A notable instance occurred in the UK, where deep fake audio was introduced as evidence in a custody battle, depicting a father as threatening. The critical concern arises in ensuring the authenticity of video, images, or audio evidence presented in legal proceedings, especially given the increasing sophistication of deep fake technology.[16]

4. LEGAL IMPLICATIONS OF DEEPFAKE

Despite the use of a technology that creates contents that closely resemble genuine images and has a big potential to create chaos and crime, current legal frameworks are still not good enough for solving the problem in the EU.

Various countries, such as India, Scotland, and the USA, have enacted laws related to information technology and data protection, criminalizing the sharing of intimate or private images online without consent. Despite these legal measures, the global proliferation of deepfake technology poses a widespread challenge that transcends borders.Dealing with the transnational nature of these crimes presents a significant hurdle, necessitating a coordinated international approach. Existing legal avenues, such as copyright protection, privacy infringement regulations in cyberspace, or defamation actions, offer only limited effectiveness and may not fully achieve their intended purposes. Once a malicious deepfake video is uploaded to the internet, eradicating all copies from the digital space becomes an exceedingly difficult task.[17]

In the current legal framework, in the US both federal and state laws, encompassing civil and criminal domains, are insufficient to prevent or remedy the harms caused by deepfakes, with the First Amendment complicating regulatory efforts.However, there is a need to be dealt with under existing U.S. law such as defamation, copyright infringement, pornography, and harassment. [18]

On the other hand, in the EU the GDPR(General Data Protection Right) that brings consent obligation for using personal data of data subjects, the European Convention on Human Rights that allows public figures to demand their privacy right to protect their name and reputation while the expectation of more tolerative, and Digital Services Act (DSA) that rules providers are obligated to take action only when there are indications that the content is unlawful, placing a significant burden on citizens or trusted flaggers.[19]

[15] Frederick Mostert & Sheyna Cruz, ''Image rights in the digital universe'', in Journal of Intellectual Property Law & Practice, XVII, No.7, 2022, p. 7

[16] Francesca Palmiotto, ''Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective'', 2023, p.1

[17] Madhura Thombre, "Deconstructing Deepfake: Tracking Legal Implications and Challenges," in International Journal of Law Management & Humanities, IV, 2021, p. 2271

[18] Lindsey Joost, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in University of Florida Journal of Law and Public Policy, XXXIII, No.2, 2023, p. 320

[19]Bart van der Sloot & Yvette Wagensveld, "Deepfakes: Regulatory challenges for the synthetic society," in Computer Law & Security Review, XLVI, 2022, p. 9

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-762-3

Lastly, The AI Act[20] which was proposed by the European Commission, the first regulation on AI in April 2021 defined the deepfake as a ''limited risk'' AI system. Article 52 of the AI Act regulates when an AI system creates deep fake content or manipulates text for public information, the deployers must disclose that it's artificially generated, unless authorized by law for criminal investigations. The disclosure should be clear and provided during the first interaction. These rules do not override existing laws, and an AI Office will encourage codes of practice for detecting and labelling artificially generated content, subject to approval by the Commission.

It is uncertain if this regulation will be a concrete solution for the deepfake threat. The effectiveness of disclosure requirements for deepfakes relies on robust enforcement mechanisms and underscores the challenge of balancing transparency with potential restrictions on artistic expression. Also, despite being currently classified as "limited risk" under the AI Act, the harmful impacts of deepfakes warrant reconsideration, advocating for their classification as high-risk AI systems.

4.1. Privacy and Data Protection Law

If deepfake technology generates video content portraying an individual in private situations they would never willingly share publicly, and if this synthetic content is virtually indistinguishable from authentic material, the affected individual may argue that the impact on them is akin to a genuine invasion of privacy. Currently, deepfake technology is exploited to create non-consensual pornographic content featuring celebrities, violating their likenesses without consent. This raises concerns as obtaining and distributing such explicit footage previously required filming the individual without their consent, constitutes a clear invasion of privacy. The use of deepfake technology intensifies the ethical and legal challenges associated with privacy breaches and unauthorized exploitation of individuals.[21]

However, there are five borderline areas that pose challenges to existing regulations. Firstly, deepfakes can facilitate live anonymous conversations, complicating issues of identity. Secondly, the General Data Protection Regulation (GDPR) does not apply to deceased individuals, allowing for the creation of deepfakes involving historical figures without falling under data protection laws. Thirdly, deepfakes about organizations and states are exempt from GDPR regulations. Fourthly, when deepfakes merge images or voices of multiple persons, it remains unclear whether the final result qualifies as personal data. Lastly, the creation of entirely fictitious persons through deepfake technology raises concerns about the scope of personal data and the household exemption. Also, the household exemption also presents challenges, as certain deepfake applications, such as revenge scenarios, fall outside the scope of GDPR coverage, highlighting potential gaps in legislative frameworks.[22]

4.2. Intellectual Rights

In April 2020, the YouTube creator Vocal Synthesis faced the first copyright claim for deepfaked audio content. The contested videos involved AI-generated voice impersonations of Jay-Z rapping Shakespeare and Billy Joel's songs. Jay-Z's legal team issued a DMCA takedown notice, arguing the unauthorized use of AI to mimic his voice. Initially removed by YouTube, the claim

[20] Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Brussels, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[21] Francesco Stellin Sturino, ''Deepfake Technology and Individual Rights'', in Social Theory and Practice, XLIX, No.1, 2023, p. 164

[22] Bart van der Sloot & Yvette Wagensveld, "Deepfakes: Regulatory challenges for the synthetic society," in Computer Law & Security Review, XLVI, 2022, p. 9

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-997-9

proved unsuccessful, and the videos were reinstated due to insufficient grounds. The incident highlighted the limited applicability of copyright law in addressing deepfake issues, as a person's general appearance or sound is typically not copyrightable, and fair use doctrines may provide a First Amendment which guarantees freedoms concerning religion, expression, assembly, and the right to petition defense for transformative content like deepfakes. The text underscores that copyright protection primarily applies to the creator of source material, making it challenging for deepfake subjects to claim infringement unless they own the content used in the deepfake creation.[23]

On the other hand, addressing the unwanted use of an individual's image through deepfake technology can be approached through legislative and legal measures. Some U.S. states, such as California, Texas, and Virginia, have enacted specific deepfake legislation, criminalizing actions like non-consensual pornography and deceptive political videos. Additionally, existing image rights laws may be updated to encompass deepfake instances; for example, New York amended its Civil Rights Law to include wholly computer-generated digital likenesses under post-mortem publicity rights. Deepfake litigation will necessitate applying established case law principles, with precedent evolving to adapt to new technologies. Notably, in a case involving video game depictions of college athletes, the 'transformative use' defense was not applicable when the portrayal aimed for realistic likeness. Claimants against deepfake misuse may draw analogies from the treatment of video games as expressive works subject to image rights, demonstrating the evolving nature of image rights law to confront challenges posed by emerging technologies.[24]

4.3. Tort Law

Defamation law is relevant to the threat posed by deepfakes, as the technology allows anyone's image to be manipulated, potentially causing significant harm to reputations. However, establishing defamation liability requires proving the publication of false and defamatory content. As the quality of deepfakes advances, verification of falseness may become challenging and require sophisticated technology. Deepfakes explicitly labeled as such, or presented as parody, may be protected from defamation claims, as disclaimers negate the assertion of factual accuracy. Drawing on the precedent set by the Supreme Court case Hustler v. Falwell, where a satirical ad with a disclaimer was deemed immune from defamation liability, deepfake creators can argue that their content is a form of parody and not to be taken as factual statements.[25]

5. SOLUTIONS FOR DEEPFAKE

5.1. Legal Solutions

The evolving landscape of technology demands a re-evaluation and expansion of legal definitions pertaining to rights, infringements, crimes, and punishments. As it stands, the current legal framework falls short in addressing issues related to emerging technologies like deepfakes, primarily due to the inadequacy of existing definitions and scopes for copyright infringements.[26]

---

[23] Lindsey Joost, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in University of Florida Journal of Law and Public Policy, XXXIII, No.2, 2023, p. 323-324

[24] Frederick Mostert & Sheyna Cruz, ''Image rights in the digital universe'', in Journal of Intellectual Property Law & Practice, XVII, No.7, 2022, p. 8

[25] Lindsey Joost, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in University of Florida Journal of Law and Public Policy, XXXIII, No.2, 2023, p. 322

[26] Chochia, Archil; Sicat, Eden Grace Niñalga (2023). Ethics and Modern Technologies: Example of Navigating Children's Rights in an AI-Powered Learning Environment. In: Ramiro Troitiño, D.; Kerikmäe, T.; Hamuľák, O. (Ed.). Digital Development of the European Union. (129−141). Springer, Cham. DOI: 10.1007/978-3-031-27312-4_9; Chochia, A.; Nässi, T. (2021). Ethics and Emerging Technologies – Facial Recognition. IDP Revista de Internet Derecho y Política, 34, 1−12. DOI: 10.7238/idp.v0i34.387466; Joamets, K.; Chochia, A. (2021). Access to Artificial Intelligence for Persons with

There is a pressing need for a comprehensive understanding of AI, guided by the expertise of scientists, to inform a regulatory overhaul that aligns with the intricacies of artificial intelligence.[27]

Moreover, it is essential to establish AI-specific regulations that parallel the pace of advancements in technology, similar to regulatory frameworks in other domains affected by emerging technologies. These regulations should extend across jurisdictions, recognizing the global nature of the internet and the rapid dissemination of content. Striking a balance between the potential threats and benefits of AI is crucial, necessitating a careful consideration of the ethical and legal implications. This involves a delicate calibration of the rights of individuals and the continued development of technology, ensuring that legal safeguards are in place to mitigate risks while fostering innovation responsibly. In essence, the law must adapt to the challenges posed by AI, taking into account its unique characteristics and impact on society.

It might be considered that these solutions are long-term strategic mindsets for the framework of a new legal system in the world of AI. Therefore, here are some short-term legal solutions to find out a legal way to protect rights of people against the threats of deepfakes:

First solution might be a legal arrangement similar to the Digital Millennium Copyright Act (DMCA) which empowers the proprietor of intellectual property to petition hosting platforms for its removal. By complying with such requests, hosting platforms are relieved of liability.[28]

Additionally, exploring "marketplace solutions" as alternative strategies for controlling the creation and distribution of Deepfakes without solely relying on individual rights as a basis for regulation might be a short-term solution.[29]

On the other hand, an offer for a regulation that would prohibit the online dissemination of deepfake content, comparing it to the unauthorized online release of intimate videos. It suggests that the inability to permanently remove such content from the internet causes significant mental, emotional, and physical harm, justifying the need for prohibition without requiring an intent to harm. The proposed regulation would classify sending personal deepfakes as online publication, encompassing both real private videos and computer-generated deepfakes.[30]

Lastly, a legal regulation similar to Virginia state law which includes deepfakes in the category of "falsely created" images and videos, making their distribution a misdemeanor might be a solution to solve pornographic contents that are made by deepfake technology.[31]

5.2. Technical Solutions

Even if the legal regulations are good enough, the law is not a convenient way to stop the viraling of the contents that are made by deepfake fastly and effectively. For this reason, while the current legal system is improving, it needs to find technical solutions to cease spreading the contents.

The forefront of deepfake technology research emphasizes the use of AI detectors, with the past two years witnessing a concentrated effort to develop automated tools for detection. Various

Disabilities: Legal and Ethical Questions Concerning the Application of Trustworthy AI. Acta Baltica Historiae et Philosophiae Scientiarum, 9 (1), 51−66. DOI: 10.11590/abhps.2021.1.04.

[27] Mazur, V.; Chochia, A. (2022). Definition and Regulation as an Effective Measure to Fight Fake News in the European Union. European Studies: The Review of European Law, Economics and Politics, 9 (1), 15−40. DOI: 10.2478/eustu-2022-0001.

[28] Erik Gerstner, "Face/off: 'deepfake' face swaps and privacy laws," in Defense Counsel Journal, LXXXVII, No. 1, 2020, p. 9

[29] Francesco Stellin Sturino, ''Deepfake Technology and Individual Rights'', in Social Theory and Practice, XLIX, No.1, 2023, p. 161-162

[30] Douglas Harris, '' Deepfakes: False Pornography Is Here and the Law Cannot Protect You'', in Duke Law & Technology Review, XVII, 2018-2019, p. 17, 124

[31] Mika Westerlund, ''The Emergence of Deepfake Technology: A Review'', in Technology Innovation Management Review, IX, No.11, 2019, p. 44

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-997-9

techniques, such as analyzing eye blinking, face warping artifacts, heart rate estimation, and facial regions, have been proposed to ensure reliable results. However, a recent survey indicates that detection methods are still in an early stage, lacking generalization capability. Current challenges arise from the opacity of many deep fake detectors, which rely on machine or deep learning techniques, leading to algorithmic opacity. This opacity raises concerns about the introduction of potentially unreliable methods, known as "junk science," into criminal trials. Suggestions for addressing these concerns center on transparency and interpretability. [32]

Another solution that is offered is banning the use of these videos on their platforms by websites. Some websites, including Pornhub and Reddit, have taken measures such as removing deepfake content, with the former relying on user reports and the latter deleting the subreddit where deepfakes originated; additionally, platforms like Discord, Gyfeat, and Twitter have specified a prohibition on face-swap porn without universally banning deepfake videos[33].

CONCLUSION

In conclusion, deepfake technology, an intricate form of synthetic media crafted through artificial intelligence (AI), introduces a spectrum of both advantages and challenges. On the positive spectrum, deepfakes demonstrate potential applications in diverse fields such as gaming, entertainment, language accessibility, medicine, and business, underscoring their capacity to contribute positively to societal advancements. However, the substantial threats associated with deepfakes, such as non-consensual exploitation, the erosion of truth, and the creation of new avenues for deception and fraud, cannot be overlooked.

The legal ramifications of deepfake technology, especially concerning privacy, intellectual property rights, and tort law, are intricate and present formidable challenges within existing legal frameworks. While certain jurisdictions have enacted specific legislation targeting deepfakes, the legal landscape remains in a state of evolution, necessitating comprehensive regulations to effectively address the multifaceted issues arising from this transformative technology. A critical emphasis is placed on the urgent need for clearly defined terms, rights, and corresponding penalties, alongside the establishment of AI-specific regulations tailored to the unique characteristics of deepfake technology.

In response to the challenges posed by deepfakes, various technical solutions, including AI detectors, are emerging to counteract the proliferation of deceptive content. However, challenges persist, notably in terms of algorithmic opacity and the potential introduction of unreliable methods into legal proceedings. As the deepfake landscape continues its evolution, a balanced approach that integrates legal, technical, and ethical considerations becomes imperative. This approach is essential for mitigating risks associated with deepfake technology while harnessing its positive potential responsibly and ethically.

BIBLIOGRAPHY

1. BROWN, Nina I., ''Deepfakes and the weaponization of disinformation'', in *Virginia Journal of Law & Technology,* XXIII, No.1, 2020, p. 1-59
2. CALDERA, Elizabeth, ''Reject the evidence of your eyes and ears: deepfakes and the law of virtual replicants'', in *Seton Hall Law Review*, L, No.1, p.177-206.
3. CHOCHIA, A.; NÄSSI, T. (2021). Ethics and Emerging Technologies – Facial Recognition. IDP Revista de Internet Derecho y Política, 34, 1−12. DOI: 10.7238/idp.v0i34.387466.

[32] Francesca Palmiotto, ''Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective'', 2023, p.8

[33] Elizabeth Caldera, ''Reject the evidence of your eyes and ears: deepfakes and the law of virtual replicants'', in Seton Hall Law Review, L, No.1, p.189

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-762-3

4. CHOCHIA, ARCHIL; SICAT, EDEN GRACE NIÑALGA (2023). Ethics and Modern Technologies: Example of Navigating Children's Rights in an AI-Powered Learning Environment. In: Ramiro Troitiño, D.; Kerikmäe, T.; Hamuľák, O. (Ed.). Digital Development of the European Union. (129−141). Springer, Cham. DOI: 10.1007/978-3-031-27312-4_9.
5. European Commission. (2021, April 21). *Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
6. GERSTNER, Erik, "Face/off: 'deepfake' face swaps and privacy laws," in *Defense Counsel Journal,* LXXXVII, No. 1, 2020, p.1-14
7. HARRIS, Douglas, '' Deepfakes: False Pornography Is Here and the Law Cannot Protect You'', in *Duke Law & Technology Review*, XVII, 2018-2019, p. 99-128.
8. JOAMETS, K.; CHOCHIA, A. (2021). Access to Artificial Intelligence for Persons with Disabilities: Legal and Ethical Questions Concerning the Application of Trustworthy AI. Acta Baltica Historiae et Philosophiae Scientiarum, 9 (1), 51−66. DOI: 10.11590/abhps.2021.1.04.
9. JOOST, Lindsey, '' The place for illusions: deepfake technology and the challenges of regulating unreality'', in *University of Florida Journal of Law and Public Policy*, XXXIII, No.2, 2023, p.309-332
10. KERNER, Catherine & RISSE, Mathias, "Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds," in *Moral Philosophy and Politics*, VIII, No.2, 2020, p. 81-108
11. MAZUR, V.; CHOCHIA, A. (2022). Definition and Regulation as an Effective Measure to Fight Fake News in the European Union. European Studies: The Review of European Law, Economics and Politics, 9 (1), 15−40. DOI: 10.2478/eustu-2022-0001.
12. MOSTER, Frederick & CRUZ, Sheyna, ''Image rights in the digital universe'', in *Journal of Intellectual Property Law & Practice*, XVII, No.7, 2022, p.551-558
13. PALMIOTTO, Francesca, ''Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective'', 2023, p.1-12
14. See https://news.sky.com/story/tom-hanks-warns-fans-not-to-fall-for-deepfake-advert-using-his-face-12974902, Accessed 13.03.2024
15. SLOOT, Bart van der & WAGENSVELD, Yvette, "Deepfakes: Regulatory challenges for the synthetic society,", in *Computer Law & Security Review*, XLVI, 2022, p. 1-15
16. STURINO, Francesco Stellin, ''Deepfake Technology and Individual Rights'', in *Social Theory and Practice,* XLIX, No.1, 2023, p. 161-187
17. THOMBRE, Madhura, "Deconstructing Deepfake: Tracking Legal Implications and Challenges," in *International Journal of Law Management & Humanities,* IV, 2021, p. 2267-2274.
18. WESTERLUND, Mika, ''The Emergence of Deepfake Technology: A Review'', in *Technology Innovation Management Review*, IX, No.11, 2019, p. 39-52

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-606-062-997-9