SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 277-290
Open Access. Online & Print

DOI: 10.5281/zenodo. 18873553

DEEPFAKE AS AN EMERGING CRIME: A VICTIMOLOGICAL PERSPECTIVE

Dalia Kadry Ahmed Abdelaziz[1], Habiba Bhouri[2], Racha Yaghi[3]

[1]Assistant Professor of criminal law, Prince Sultan University, Saudi Arabia, dkadry@psu.ed.sa, https://orcid.org/0000-0002-7616-5827
[2]Assistant Professor of law, Prince Sultan University, Saudi Arabia, hbhouri@psu.edu.sa, https://orcid.org/0000-0001-7855-3965
[3]Assistant Professor of law, Prince Sultan University, Saudi Arabia, ryaghi@psu.edu.sa, https://orcid.org/0000-0001-6424-3675

Received: 11/11/2025
Accepted: 18/12/2025

ABSTRACT

Deepfake technology has created major threats to digital hijacking victims, including the denial of privacy, erosion of personal space, and social media abuse. This research describes deepfake as a new type of crime, and focuses on the significant psychological and social harms resulting from these technologies for its victims. This paper classifies victimization from deepfake to three general categories: non-consensual pornography; identity theft; and financial fraud; highlighting the emotional trauma and stigma that deepfaking affords victims. It also analyses the legal framework, emphazising limitations in existing legislation, that are insufficient to adequately tackle the multi-faceted risks from the misuse of deepfakes. Deeping on the literature in legal studies, psychology, and gender studies, the study builds consensus toward the prompt need for legal reforms and preventative measures. These include the development of specific laws designed to protect victims, improving education and training in digitalfield, and international cooperation across jurisdictions, to help curb the spread of threats associated with deepfaking. Finally, this paper seeks to investigate the intricate interaction of technology, law and victimhood, laying a basis for collective action in a new context of crime. At the heart of this is placing the voices and the rights of victims of crime at the forefront of a swiftly evolving digital terrain. With deepfake technology advancing, a victim-centred as well as, an interdisciplinary response is necessary to protect trust, security and human dignity in the electronic age.

KEYWORDS: Deepfake Technology, Victimology, Non-consensual Pornography, Legal Challenge, Psychological Impact.

1. INTRODUCTION

Advancements in artificial intelligence (AI) lead to deepfake technology, which is a technology that allows an individual to create extremely realistic yet falsified digital images, audio, and video. In fact, developing this technology is both a threat and a boon to victims as well as perpetrators of digital crimes. Fake media is becoming more sophisticated, and as of 2025, these tools have been weaponized against victims: defamation, financial fraud, non-consensual pornography and political disinformation. The increasing complexity and user accessibility of deepfake tools increases the threat of misuse and requires an urgent legal and ethical analysis (Januário, 2025; Ali et al., 2025; Arvitto, 2025). Recent victimological studies have emphasized, the deep psychological trauma and social stigma, those targeted with such deepfake crimes have become and on this, its impacts can transfer well beyond the digital world for them into their personal and social lives (Ali et al., 2025; Cheng, 2024). Despite the growing recognition of these personal, human rights and security threats, the existing legal regimes sometimes trails behind the tech landscape. And this gap is particularly pronounced in where there is no legislative language on the malefic use of deepfake technologies (Banfatin et al., 2024; Arvitto, 2025; Putri et al., 2024). Indonesia's own Information and Electronic Transactions Law (UU ITE) and Personal Data Protection Law (UU PDP), for example, impose regulation for digital use but they do not properly account for damages attributable to deepfakes (Arvitto, 2025). The general lack of targeted legal protection increases the chances of victimization and the lack of access to justice, as such criminal behavior is often accompanied by a range of wider societal problems, such as online sexual harassment or gender-based violence (Cheng, 2024; Hafiz, 2024). Women are disproportionately hurt, when deepfakes are used to further the current state of digital harassment and gender disparity (Ali et al., 2025; Cheng, 2024). This paper analyses deepfake technology from a victim's view and addresses its criminal, legal, and social implications. This study takes a multidisciplinary perspective and evaluates the risks of deepfakes, as well as the state of law and experiences in the digital age of crime. Since the vast development of deepfake technology, and its far-reaching impacts on people and society is emerging, legal and ethical as well as social responses will need to be formulated in a timely manner. New case reports show a disturbing spike in non-consensual deepfake pornography, financial scams and political disinformation around the globe, showing the overuse of these technologies, the terrible personal, and societal consequences they generate. So, this paper intends to help develop more potent defenses, regulations and prevention measures to the harm caused by deepfake crimes. The study aims to examine the forms of victimization experienced by victims of deepfake technology and to analyze its psychological and social impact. What are the existing gaps and challenges within existing legal frameworks that inhibit good prevention and prosecution of deepfake-related crimes? How do ethical considerations, as well as public awareness, impact the responsible usage and regulation of deepfake technology? What can integrated strategy be implemented to safeguard victims and minimize social harms stemming from deepfakes? Responses to these questions must lay the groundwork for establishing sound policy recommendations and interventions.

The methodology of this research is qualitative and analytical in nature developed on the basis of a comprehensive literature review of recent literature on deepfake technologies in legal, psychological, ethical, and social domains. In choosing the literature, we focused on peer-reviewed scholarly articles, legal literature, and case reports written since 2019, eliminating out-of-date or non-peer-reviewed materials to ensure we received new and relevant data about deepfake victimology. Based on the information gathered through desk research, the study determine to analyze related articles, international reports, and case studies focusing on victim experiences and the impacts of deepfake-related crimes. Additionally, it sought to identify gaps and challenges in legislation and regulatory frameworks addressing these crimes in various countries worldwide**.**The analysis is informed by an interdisciplinary frame that combines law, technology, psychology, and social sciences to offer an in-depth understanding of the psychological and social impacts on victims and legal shortcomings.

This comprehensive approach is designed to develop a strong knowledge base for evidence-based recommendations aimed at enhancing legal protections, supporting victims, and mitigating risks associated with deepfake misuse.

2. LITERATURE REVIEW

The rise of deepfake technology, or the creation of digital media that is hyper-realistic

but also artificial, typically created employing virtual reality methodologies, has led to ethical, legal and psychological controversies. As digital devices mature, their opportunities for abuse pose fundamental questions for individuals and cultures. This literature review is aimed at referencing the most recent literature on victimization, regulatory response and ethics associated with deepfakes.

Origins of victimological theory Victims of the past and today are based on seminal theories such as Mendelsohn's (1984) and Von Hentig's (1948) theories of victimology: which are concerned with the relationship between the victim and the offender and on identifying and categorizing types of victims to explain patterns of victimization. Having expanded upon their main victimology explanations of victim characteristics and the dynamics of victimization processes, the analysis links and extends these models to digital victimization via deepfake technologies, emphasizing new forms of mediated harm as requiring adapted theoretical frameworks.

2.1. Victimization Based On DFS

Online crime is becoming common, even more common in services that can be offered via the Internet. But there is little direct evidence of what type of data corruption/manipulation occurred (Pomeroy, 2007). As digital content is durable (Ali et al., 2025), victimization often involves sustained psychological and reputational harm that can provoke future victimization. Women's victimization has broader emotional risks as the psychological consequences of such experiences are often more severe; also, it is a very common attack on deepfake, with women being top of the total victims (Khimi et al., 2024). This shows a need to further investigate the concept of victimization and how these experiences impact the wider social effects of this technology.

2.2. Legal Challenges and Regulatory Responses

The legal basis of deepfakes remains vague, amplifying the victimization inflicted. As noted by Putra & Multazam (2024), there is no existing legal mechanism or enforcement tool when it comes to the issue of deepfake pornography, which is a serious matter especially in Indonesia. Also, a systematic review of Khimi et al. (2024), it is their calls for legislation which regulates the use of the deepfakes through serious ethical regulation rules and swift detection of deep faking. Veljković et al. (2024) likewise mentioned: the objective value of AI is dependent upon users' motives thus, complicating regulation of AI itself. Thus, call for changes in legal frameworks with emerging threats posed by synthetic media or to protect a victim's right (Iqbal et al., 2023). A comparative review of legal responses shows significant disparities across jurisdictions. For instance, while California has pioneered criminalizing non-consensual deepfake pornography, countries like Indonesia show regulatory gaps that inadequately address deepfake harms (Arvitto, 2025; Putra & Multazam, 2024). This contrast underscores the urgent need for harmonized global frameworks. Moreover, the absence of uniform international standards complicates cross-border enforcement and victim protection, highlighting the importance of global cooperation in legislative development

2.3. Ethical Concerns and Educational Needs

On the ethical concerns behind deepfakes several studies have been done. Deeply, the deepfake technology has serious uses but also raises significant ethical concerns—including financial crimes and misinformation. Given the potential for nefarious and unethical use of deepfakes, Rancourt-Raymond and Smaïli (2022) discuss ethical concerns, including fraud, blackmail, and manipulation. Accordingly, whilst deep faking generates creativity and innovation, it also creates risks that call for stricter ethical limits and education. Overall calls across studies to address digital literacy, allowing consumers to better identify the legitimacy of media content, and implement ethical frameworks for technological education (Rancourt-Raymond & Smaïli, 2022; Khimi et al., 2024).

The review of related literature reveals, that deepfake technology becomes a growing danger that ranges on much more than technical problems; it also impacts a range of individuals' psychological, social, and legal rights. Although detection and ethical responses have developed detection and ethical responses to them, there are still severe legislative and regulatory lacunae that allow many perpetrators, especially women victims of non-consensual use of image and video abuse to continue to be victimized. So, the literature emphasizes an immediate necessity to conduct comprehensive cross-disciplinary research involving law, psychology, and technology to produce robust responses that safeguard victims' rights and encourage responsible use by users of this digital tool. Grounded on this foundation, the current study takes a victimological perspective to consider the

impact of deepfakes and seeks to bridge these voids with legal, ethical, and technological recommendations to protect individuals and society.

2.4. The Evolution Of Deepfake Detection And Its Societal Impact

The evolution of deepfake content and its societal implications، create new social and computational challenges that need both detection strategies and legislative mechanisms. Deepfake art is a sensitive subject, because it is very difficult to determine between the real and false images. (Harris et al., 2024), this article focuses on the impact of deepfakes on public discourse and social interaction. This literature review reflects synthesis of existing research on deepfake detection: how it can help. It focuses on its ethical concerns; and stresses urgent yet multifaceted policy approaches necessary.

2.5. Techniques For Detecting Deepfakes

Advances in deepfake detecting technology are crucial if we are to have any prospects of recognizing or limiting the damage done by manipulated media. (Venkateswarulu & Srinagesh, 2024) point out that more transparent and explainable AI models will be necessary to enhance the accuracy of deepfake detection: as a significant technological evolution, deepfake technology leads to increased complexity of detection (Venkateswarulu & Srinagesh, 2024). Al-Khazraji et al. performed the systematic review in the same manner (2023) who identifies different means of detection, adding that successful methods would necessitate both technical and policy reforms to adequately combat the misinformation spread through deepfakes (Al-Khazraji et al., 2023). Furthermore, Nait-Ali et al. are also discussed (2023) in the context of generative adversarial networks (GANs), which have shown them to effectively create and detect deepfakes, further indicating that higher-grade detection techniques become needed to maintain the authenticity of digital communication (Nait-Ali et al., 2023).

The societal consequences of these deepfakes go far beyond solving challenges of technology; they are also breeding grounds for misinformation and distrust. In another analysis, Qureshi & Khan (2024) find that deepfaking increases the susceptibility to misinformation and deception as a result of manipulation of human cognition and emotion (Qureshi & Khan, 2024). The influence of algorithms in social media is likely to contribute to the manipulation of public discourse and trust in media sources, where algorithmic amplification of deepfake content will have significant ramifications for disinformation (Al-Khazraji et al., 2023; Sharma et al., 2023). A research (Sharma et al., 2023) emphasizes that the rapid spread of deepfake content can be extremely harmful, potentially damaging both individuals' reputations and public awareness of public norms regarding truth when it comes to the politics of disinformation (Sharma et al., 2023).

2.6. Ethical Concerns And Policy Implications

The ethical considerations of deepfakes need to be considered for the responsible use and prevention of misuse. Researchers such as Tuysuz and Kılıç (2023) call for legislative frameworks to sanction not only malicious usage of deepfake but also legitimate applications in entertainment and education (Tuysuz & Kılıç, 2023). The combination of ethics and technology indicates the need for the establishment of guidelines detailing best practices for creating and distributing deepfake applications. However, ethical norms governing the publication of deepfakes help decrease potential harms due to misinformation and deception (Li & Wan, 2023). As per the literature, the challenges posed by deepfakes need to be approached cross-culturally through a technological, ethical, and political lens. We must create legal frameworks for detection that enable protection of individuals and provide the conditions for the innovation of deepfake technology (to protect users and businesses). A balance between good detection and careful policy addressing the various risks of deepfakes can ultimately be achieved by adopting an integrated approach, focused on both creativity and social impact.

The papers on the past reviewed work indicate, that the development of deepfake technology is posing an ever-increasing challenge in detecting and identifying authentic and manipulated content. This is necessary to be addressed by the construction of more transparent and explainable artificial intelligence techniques, which make detection accuracy higher. Furthermore, deepfake media plays a big part in damaging the public trust in the media, through allowing misinformation to spread, influencing public opinion and further calls for a balancing of political and ethical response. And the phenomenon of deepfake must be tackled through the integration of technology development, legislation and ethics that protects individuals and society from misuse, but also fosters responsible use of it in education and entertainment. This study is, therefore, informed by a number of dimensions and the recommendations that can be created in order to achieve a proper equilibrium between innovation and social responsibility (Chesney & Citron, 2019;

Tolosana et al., 2020).

3. DEEPFAKE VICTIMIZATION: FORMS, CASE STUDIES, AND CONSEQUENCES

Types of victimization associated with deepfake technology in this section will be elaborated completely by looking at varieties for victimization arising from misuse deepfake tech. -specific examples and case studies will be included to help illustrate the real-world implications of deepfakes, both in the form of individual victims as well as in the context of communities.

3.1. Non-Consensual Deepfake Pornography

The most current type of victimization with deepfake (Deepfakes) is non-consensually making and sharing of explicit images/videos of a person without the person's consent known as a piece of pornography. This type of image based sexual abuse can have devastating negative implications on the mental well-being (mentality) of a survivor, their career prospects, and their social willingness. The widespread dissemination of such content online aggravates psychological trauma and reputational damage for victims (Ali et al., 2025).

Case:

In an era of social media, when all forms of deepfake pornography are online, the need for understanding victims' experiences of non-consensual pornography is pressing. Interviews with victims demonstrate that when users are exposed to deepfake pornographic content without their consent, this humiliation causes shame, anxiety, and social withdrawal, underlining the need of comprehensive legislation and support for victims (Al-khazraji et al., 2023).

3.2. Scams And Financial Fraud

Deepfake techniques are also being used into financial fraud schemes, where audio or visual alterations are made to mimic real parties or entities. Losses for victims can be substantial, with loss of reputation for both victims and companies causing irreparable harm. This type of exploitation is concerning and has implications for trust in digital communications and cybersecurity (Nguyen et al., 2022)

3.3. Political Disinformation and Reputational Collusion

Deepfakes are an effective source of political disinformation, videos that have been manipulated and have been deployed to mislead voters or discredit political figures. According to Ali et al. (2025), using all these tools maliciously may lead politicians and public figures to be subject to damage to its reputation. This includes social implications, because misinformation can change public perception, which can have devastating effects on democratic processes. Drawing on election case studies , this essay presents findings from an election cycle in which deepfake videos were shared to discredit candidates. The rapid dissemination of altered information on social media not only damaged the credibility of individual users but also brought into question the public's trust in the electoral system and media (Hoek et al., 2024).

Psychological and emotional effects were reported in 7% of the sampled individuals. The emotional impact of deepfake is heavy and typically is not considered where it resides. Research suggests victims of deepfakes have psychological burdens from anxiety and depression to PTSD (Ryu, 2024). For example, Hoek et al. (2024) demonstrate that deepfake therapy can address the trauma of victims, both showing possibilities for healing and the magnitude of the harm inflicted under digital manipulation.

Case In Point: Victim Support Efforts

Actions undertaken by advocacy organizations to assist deepfake victims in their emotional distress illustrate the necessity for open and supportive spaces. This effort is not just to offer psychological assistance, but also to inform the community about the actual situation of victims of deepfakes (Ali et al., 2025).

The data in this section indicate that victimization with deepfake is complex and requires interventions in specific directions. Knowing which non-consensual pornography, you're getting, a financial scam, political propaganda, and their psychological aftermath means there is so much to know about how to design a social safety net or policy response.

3.4. Challenges And Statistics Related To Deepfake Victimization

Expanding upon the single, community perspective upon deepfake victimization and previous support initiatives, we must investigate the overall extent and nature of deepfake defaming through the latest statistics available. These numbers serve to illustrate both how serious the issue really is, and the urgency for holistic responses. New research suggests the rate of deepfake victimisation is growing with the rapid rate of digitalization of deepfakes. More than 17,000 deepfake videos were detected

online in 2022 (Sensity AI, 2022) (Chesney & Citron, 2019), of which 96% are nonconsensual pornographic content to individuals, and women in particular. In addition, a 2023 research conducted in California on non-consensual deepfake material indicated that 15% of users were struggling to cope with severe psychological symptoms including anxiety and depression, and long-term impact on their social and professional life .At the financial level, cybersecurity reports show that deepfake-enabled fraud attacks increased by 250 percent between 2021 and 2023, with the result that hundreds of millions of dollars disappeared between these two incidents .In terms of politics, several documented cases in various countries of deepfake disinformation led to a 30% reduction in public trust (Pew Research Center, 2023). These statistics stress the urgent need for effective measures to counter emerging technologies: legislation, public education, psychological support for victims and the development of detection technology.

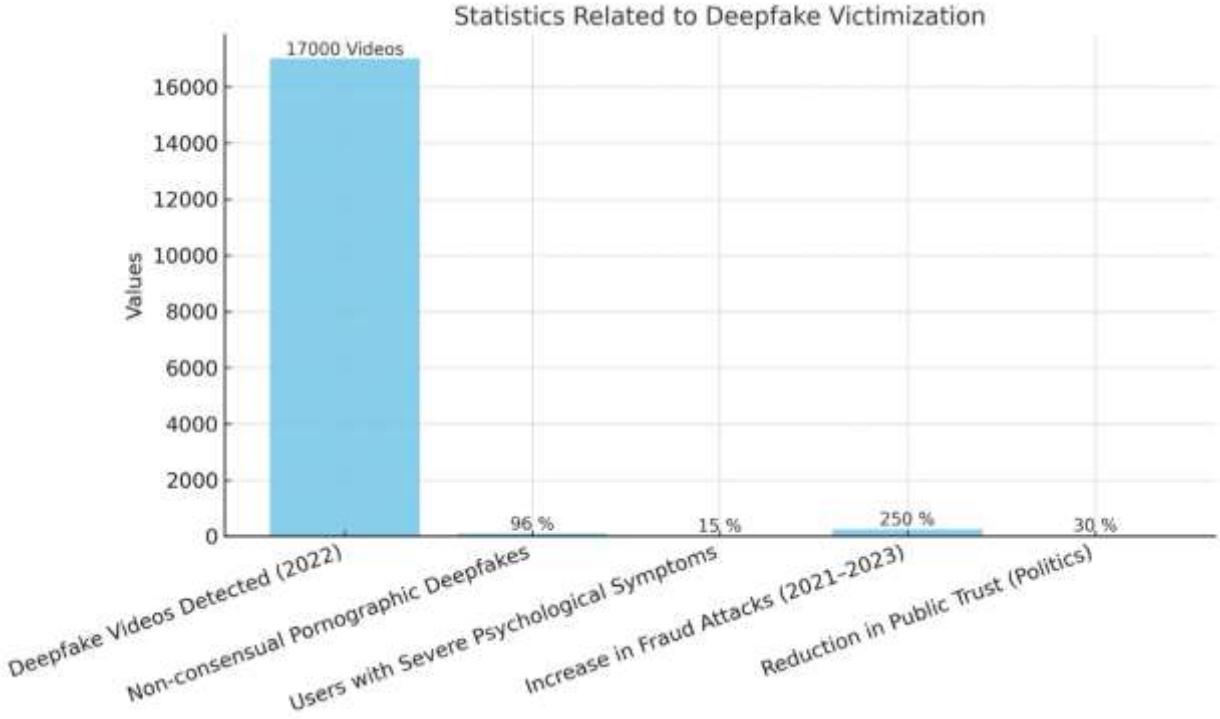

Figure 1: This Figure Demonstrates The Dramatic Scaling Of The Threats Around Deepfakes Over Time. The First Line Indicates How Many Deepfake Videos Are Being Estimated Online; The Second Line Denotes The Percent Of All Fraud Attempts Made Involving Deepfakes, And The Third Line Indicates What Organizations Are Directly Targeted By Deepfake Fraud.

4. SOCIAL, PSYCHOLOGICAL, AND ECONOMIC IMPACTS OF DEEPFAKE TECHNOLOGY

Beyond this segment are social impacts on media, democracy, the wellbeing of the individual and economic opportunity brought by deepfake technology. These impacts are laid out in subsections that rely on case studies and current research to illustrate the scale of the challenges posed by deepfakes.

4.1. Decline Of Confidence In Media.

As deepfakes spread throughout society, news users have not only become increasingly skeptical of political institutions but have also grown more distrustful in general of the media and the institutions it serves. Certainly, in doing so, the campaign sells the deception not from the misinformation itself, but from the framing of the lie—that is, the digital trap of a "fake news" video. This is the case in political disinformation campaigns. When we look at video images during electoral cycles, deepfakes demonstrate how their fabrication can erode public confidence in elections. Throughout the United States presidential election in 2020, deepfakes were used to spread disinformation to discredit candidates influencing voting decisions. At the very least, they had a deleterious impact on the integrity of the elections (Vaccari & Chadwick,

2020). When it comes to deepfaking technology's psychological implications, this debasement of public trust in the media sets in motion deeper consequences, especially affecting direct victims of deepfakes.

The proliferation of deepfake videos not only leads to distrust of certain media outlets but also creates a generalized skepticism that affects audiences' belief in even reputable sources. This erosion of trust creates fertile ground for conspiracies and disinformation to take hold, sapping media of its function as an intermediary. In the U.S. presidential election, multiple such deepfake videos were spread to discredit candidates, generating greater public confusion and skepticism (Vaccari & Chadwick, 2020). Further, research highlights that greater awareness of deepfakes may paradoxically increase voter skepticism toward the electoral system itself, reducing political participation and engagement (Ternovski, Kalla, & Aronow, 2022). Moreover, the widespread use of fake news and manipulated content on social platforms also serves to diminish audience trust in traditional news sources (Guess, Nagler, & Tucker, 2020). The accumulation of these effects leads to political disengagement, polarization, and distrust in institutions, thus undermining how democracy really works.

This erosion of public trust underscores the urgent need for comprehensive strategies combining technological, legal, and educational measures to counter the threats posed by deepfake media.

4.2. Psychological Impacts On Individuals

Deepfakes can also be harmful psychologically and have damaging impacts on victims simply because of what they have consumed. Ruvalcaba and Eaton (2020) showed that victims often experience severe emotional distress that leads to long-term mental health issues such as anxiety and depression. This showcases the wider health consequences of this type of manipulated sexual material, especially for women. Research has found that victims of non-consensual deepfake pornography have worse psychological well-being and somatic symptoms than non-victims. Many of these survivors sustain emotional and psychological pain, which underscores the pressing demand for support services and strengthened legal protections (Ruvalcaba & Eaton, 2020). In addition to the individual psychological harm, deepfakes also endanger democratic institutions by spreading misinformation that undermines public trust and political engagement (Ternovski et al., 2022).

4.3. Political Manipulation and Misinformation

Deepfake political content poses serious threats to democracy by spreading misinformation and manipulating elections. Ternovski et al. (2022) demonstrated that exposure to deepfake information paradoxically reinforces voters' skepticism toward the electoral system. Media manipulation has caused considerable changes in public opinion, political discussions, and voter behavior, posing a grave threat to people's trust in government. Campaigns utilizing deepfakes produce a public that is more skeptical and less politically active, which, over the long term, may negatively affect participatory democracy (Ternovski et al., 2022).

4.4. Economic And Legal Implications

The rapid growth of deepfake technology raises significant business and legal concerns. Saxena and Grewal (2024) point out that deepfakes have become tools for social engineering and financial fraud, representing a considerable cyber threat. The absence of coherent international legal frameworks makes ongoing efforts to address these risks more difficult. In particular, legal issues faced by organizations, especially in finance and public relations, remain widespread problems. Preventative measures, such as training and knowledge management, can empower workers to identify tampered content and minimize harm (Saxena & Grewal, 2024).

The social consequences of deepfake technology demonstrate that these challenges are not black and white. They range from loss of credibility in the media and democratic processes to psychological harm inflicted on individuals, as well as economic risks to both organizations and society at large. Addressing the social, technological, and political consequences of this emerging technology requires a layered series of interventions. These include innovations in technology, reforms in criminal justice, and enhancement of human rights and public education efforts. Such integrated approaches serve as vehicles to restore trust in public and private institutions and promote democratic integrity

5. RECOMMENDATIONS TO SOLVE THIS PROBLEM DUE TO DEEPFAKE EFFECT

Considering the development of deepfake technology and huge concern for individuals and society, this part offers guidance on legislative systems and policy directions designed to minimize the negative effects related to these technologies. The recommendations are arranged in four subsections, dealing head on legislative actions, corporate accountability, public publicity, and global cooperation.

5.1. Legislative Measure.

The essential step to a comprehensive response to the new problem of deepfake technology should be the passage of robust laws. The Suggested legal reforms include Criminalization of Malicious Deepfake Use: Establish laws that specifically criminalize the creation and distribution of deepfakes intended for harm, such as non-consensual pornography or disinformation campaigns. These laws would empower police to take decisive action against offenders (Li & Wan, 2023; Hägle et al., 2024). Privacy Protections: Implement comprehensive privacy laws giving the people with their likeness and personal data complete independence. The risks showed by deepfake technology to personal image rights and consent must be addressed in these types of reforms, such that informed consent has significant value when considering media representation. Example: Legislative Initiatives. Recent proposals in states such as California to regulate "revenge porn" and non-consensual deepfakes offers a template for how to address these legal matters. Policymakers can use these models as an early template to broader legislative interventions (Davis & Fors, 2020).

5.2. Corporate Responsibility and Ethical Standards

Technology companies are responsible for handling this type of deepfake and need to be accountable for ethical application. Recommendations include:

Design of guidelines: Companies should adopt guidelines for ethical use and production of deepfake technology. This entails encouraging transparency and obtaining users' informed consent before images or voices are altered (McCosker, 2022; Yadlin-Segal & Oppenheim, 2020). Integration of Detection Innovations: Invest in and promote cutting-edge detection technologies identifying deepfake content before it proliferates. Partnering with academic and tech institutions could lead to the development of more effective tools to help counter misinformation practices (Alhaji et al., 2024; Ruiter, 2021).

By integrating education methods with a model approach, researchers can create the systems themselves that are effective in changing the misinformation market. These standards would be a reference point for ensuring accountability in the technology industry, with the responsible exploitation of deepfake technology (Ruiter, 2021).

5.3. Raising Awareness and Teaching Digital Literacy

Raising awareness of the complex — and dangerous — nature of deepfakes is just as much a part of the job. Recommendations include:

Educational Campaigns: Launch public awareness campaigns focused on the presence of deepfakes, the potential consequences, and how people can spot manipulated material. Educational programs are also strong vehicles to spread digital literacy since people are taking seriously the media they consume (McCosker, 2022; Khimi et al., 2024). Law Enforcement and Legal Practitioner Training: Conduct training to educate officers, lawyers and courts on the implications of deepfake technology and the challenges for prosecuting the offense (Hoek et al., 2024). Example Programs: Community Engagement. Media literacy programs developed by NGOs and academic institutions can help communities have a better understanding of how deepfake technology works and the components of the technology and help communities engage with critical literacy for media (Alhaji et al., 2024).

5.4. International Collaboration

The global character of technology highlights that there is more than sufficient need for an international collaboration in addressing the problems posed by deepfake technology. Implications for industry and public health are many ranging from:

Systematic reform of regulatory norms on deepfakes will encourage countries to adopt similar protective measures. This will enable more international cooperation in enforcing laws to solve the problems of this kind, in practice (Afchar et al., 2023). International organization, e.g. United Nations to work with the United Nations for global campaigns on misinformation and protecting the public from the challenges of deepfake (Clark &

Lewandowsky, 2025; Ahmed et al., 2023). Conclusion. The challenges of extreme deepfake technology call for a global approach: legislation, corporate responsibility, public education, and cooperation between government, the public, and academia. Maintaining the partnership between policymakers, technology developers, civil society and international institutions will be crucial to adapting and updating these measures — and making sure that deepfake technology is being properly utilized and not harmful to society.

6. SUGGESTIONS FOR FUTURE RESEARCH OR POLICIES ABOUT THE USE OF DEEPFAKE TECHNOLOGY

The section further discusses, below general guidelines, several specific suggestions for future investigations or policy efforts in deepfake.

6.1. Enhancement Of the Legal Systems

Legislation needs to be improved to prevent any misuse of deepfake technology from occurring. Policymakers should:

- Establish Specialized Laws: Make specific laws banning evil deepfakes as for example, non-consensual porn and identity theft. Such regulations should specify the forbidden conduct and punishment and must distinguish malicious intention so as to avoid hindering legitimate exploitation (Qureshi & Khan, 2024).
- Promote Global Co-operation: With the growing digital content, it becomes an essential part of country to work together to work towards the establishment of standard legal systems and common standards to challenge the abuse of misinformation and deepfake all around the world.

6.2. Development Of Detecting Technologies

The investment in advanced detection models is necessary to reduce the risks generated by deepfake technology. Novel research stresses the need for lightweight and effective deep learning models for real-time video analysis. Models such as LW-DeepFakeNet, which contain convolutional neural networks and LSTM layers, have given good results to detect manipulated content very quickly (Masud et al., 2023). Ongoing improvements in machine learning and computer vision systems are necessary to offer adaptive feedback, thus enhancing the efficiency of detection systems when confronting the current trend in deepfake threats (Caci et al., 2024). Moreover, cybersecurity knowledge is critical for improving detection algorithms as evasion techniques become more complex.

6.3. Promoting Ethical Standards

Ethics underpin the responsible use and construction of deepfakes. Recommendations include:

- Create ethical guide: Create an ethical framework, with a robust base ethic, including ethicists, technologists, lawyers and legal experts working collaboratively with other disciplines.
- Increasing Public Awareness: create public campaigns to lecture the public about the risks of deepfakes, encouraging digital literacy, so that members of the public could critique media content for malicious intent.

6.4. Support For Various Collaborations

Deepfake challenges require cross-sector collaboration. Key actions involve:

- Encourage Research Partnerships — Promote cross-cultural and interdisciplinary research among scholars in law, technology, social science and creative fields so that researchers can explore the real-world impact of deepfake.
- Developing Stakeholder Conversation: Encourage stakeholders to talk with policymakers, technologists, educators, and advocates to create holistic and inclusive policies.

The challenges of deepfake technology depend upon collective action, working through legal reform, technologic innovation, ethical governance, and interdisciplinary collaboration. To find solutions that are flexible; to protect privacy, trust, and the digital age, scholar must continue to conduct research, engaging the public, and foster global efforts.

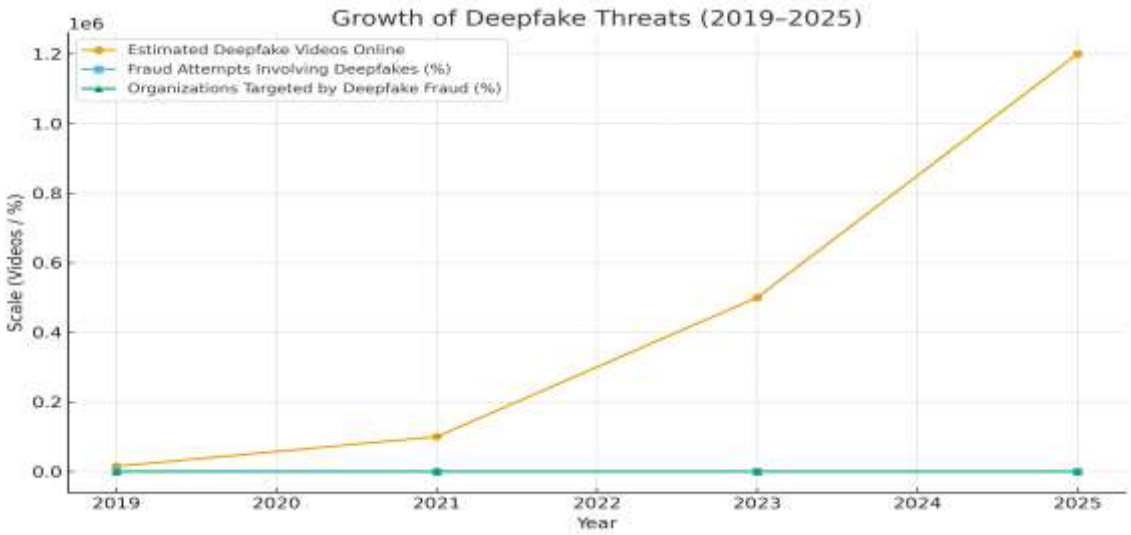

Figure 2: This Figure Illustrates the Rapid Growth of Deepfake-Related Threats Over Time. The First Line Shows the Estimated Number of Deepfake Videos Online; The Second Line Indicates the Share of Fraud Attempts Involving Deepfakes; The Third Line Represents the Proportion of Organizations Targeted by Deepfake Fraud.

7. CONCLUSION

This work has identified variants of deepfake technologies with the emergence of victimization forms that stem specifically from its misuse – such as non-consensual pornography, financial fraud, or political disinformation. Thus, these findings need to be supported with the principles of policies that mitigate not only the harms of personal identity to these individuals but also foster innovation and ethical norms. It also indicates how public awareness campaigns should be implemented to avoid misuse of deepfakes and protect social trust (Ali et al., 2025; Talib et al., 2023). In the meantime, it is technologists and researchers who, in a continuous cycle, design detection techniques and develop solutions that are ethical (such as privacy) and public domain friendly (Cheng, 2024; Hailtik & Afifah, 2024). Because deepfake is changing rapidly technologically, it is vitally needed that continued research continues. Future work should sharpen detection methods, probe the psychological and social impact of deepfakes, and create comprehensive legal and ethical frameworks. Cross-disciplinary collaborations among law, technology and social science scholars will be necessary to manage the complex problems associated with deepfake (Mania, 2022; Kasita, 2022; Tuysuz & Kılıç, 2023; Khare & Raghuwanshi, 2025). Taking place in a broader system, we need to consider the effects of Deepfake Technology in several ways. On the one hand there is technological progress; on the other legal reform; ethical governance methods; and public involvement. Such collective measures are critical if we hope to protect privacy, trust and security in a world increasingly defined by generative AI technologies.

8. RECOMMENDATIONS ON FUTURE STUDIES

In order to face the diverse challenges of deepfake technology, targeted and broad-based research is urgently required. This passage describes significant areas of future research, illustrating these from experiences on the ground and providing practical suggestions for public policy, training, and academic teaching.

Recent research has already shown the potential strength of the system and showed that by using multimodal information (audio, video, metadata), our ability to detect deepfakes will increase significantly as well (Nguyen et al., 2019). Real-time detection is crucial for live-streamed content, particularly in our current social media era, where deepfaking can spread very fast. A further effort aimed at stimulating innovation here is Facebook's Deepfake Detection Challenge, a challenge that encourages the build-up of scalable, real-time approaches (Dolhansky et al., 2019).

8.2. Improvements In Legal Framework

Deepfake technology is undercutting legal systems globally. Research should concentrate on:

In-Depth Analyzing Global Approaches:

A comparison of various countries to regulate

deepfakes can show both positive strategies and some gaps that need to be filled. California's move to criminalize nonconsensual deepfake pornography is not only a paradigm of victim preservation, but a model that so many other jurisdictions have not yet come along (Citron & Chesney, 2019).

Victim Support: Aside from punishing offenders, new laws have to do with victim support – counseling, expedited decision-making by the courts. It has also been shown that deepfake technology has negative psychological effects on victims that require significant protections and education (West et al., 2020).

8.3. Ethical Standards And Public Awareness

The design of ethical requirements is crucial for the ethical criteria for deepfakers and distributors of such information. There are also guidelines available from the IEEE Global Initiative on the Ethics of Autonomous and Intelligent Systems which can be used in the context of deepfakes (IEEE, 2019).

Targeted Educational & Awareness Campaigns: Media messages need to be specific and tailored to diverse audiences. Interpreters and professionals working with these issues benefit from broad discussions. Research shows that combining media literacy with strong community support leads to better engagement with misinformation.

8.4. Interdisciplinary Collaboration And Inclusivity

This type of convergence on technology, ethics, and society is what MIT aims to implement as part of its partnership with the Partnership on AI (Partnership on AI, 2021). It is therefore necessary to carry out research in marginalized and vulnerable communities who are more adversely affected by deepfakes. Policies and technologies should accordingly be adapted to all cultural and socio-economic contexts.

Policymakers, technologists, educators, and civil society must proactively collaborate to build adaptive, equitable, and transparent policies. In an age of synthetic media more prevalent than ever, it is this joint effort that will be necessary to protect both individuals and society.

Acknowledgements: The authors would like to express sincere gratitude to Prince Sultan University, Riyadh, Saudi Arabia, for its invaluable support and resources. special thanks to the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for their financial and academic support to conduct this research and publish it in a reputable Journal.

Ethics Declarations: Ethics approval for this research was obtained from Prince Sultan University's Ethics Review Committee. The study adheres to the ethical standards set by the university and complies with international ethical guidelines for research involving human subjects. All data collected were handled with strict confidentiality.

Competing Interests: The authors declare no competing interests.

REFERENCES

Afchar, D., Hennequin, R., & Guigue, V. (2023). Of spiky svds and music recommendation. 926-932. https://doi.org/10.1145/3604915.3608850

Ahmed, S., Ng, S., & Bee, A. (2023). Understanding the role of fear of missing out and deficient self-regulation in sharing of deepfakes on social media: Evidence from eight countries. *Frontiers in Psychology, 14*. https://doi.org/10.3389/fpsyg.2023.1127507

ales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131-148. https://doi.org/10.1016/j.inffus.2020.06.011

Alhaji, H., Çelik, Y., & Goel, S. (2024). An approach to deepfake video detection based on aco-pso features and deep learning. Electronics, 13(12), 2398. https://doi.org/10.3390/electronics13122398

Ali, M., Fernando, Z., Huda, C., & Mahmutarom, M. (2025). Deepfakes and victimology: Exploring the impact of digital manipulation on victims. *Substantive Justice International Journal of Law, 8*(1). https://doi.org/10.56087/substantivejustice.v8i1.306

Al-khazraji, S., Saleh, H., Khalid, A., & Mishkhal, I. (2023). Impact of deepfake technology on social media: Detection, misinformation and societal implications. *The Eurasia Proceedings of Science*

Technology Engineering and Mathematics, 23, 429-441. https://doi.org/10.55549/epstem.1371792

Arvitto P., Medan, K., & Fallo, D. (2024). Pengaturan hukum pidana di indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. pk, 2(1), 60-73. https://doi.org/10.62383/pk.v2i1.402

Arvitto, R. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia, 4*(2), 73-82. https://doi.org/10.35912/jihham.v4i2.3937

Banfatin, P., Medan, K., & Fallo, D. (2024). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. *PK, 2*(1), 60-73. https://doi.org/10.62383/pk.v2i1.402

Brüggemann, U., Hitz, J., & Sellhorn, T. (2012). Intended and unintended consequences of mandatory IFRS adoption: A review of extant evidence and suggestions for future research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1684036

Caci, B., Giordano, G., Alesi, M., Gentile, A., Agnello, C., Presti, L., … & Monzani, D. (2024). The public mental representations of deepfake technology: An in-depth qualitative exploration through Quora text data analysis. *PLOS ONE, 19*(12), e0313605. https://doi.org/10.1371/journal.pone.0313605

Cheng, X. (2024). The gendered impact of deepfake technology: Analyzing digital violence against women in South Korea. *Lecture Notes in Education Psychology and Public Media, 75*(1), 80-85. https://doi.org/10.54254/2753-7048/75/20241102

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753-1819. https://doi.org/10.2139/ssrn.3213954

Clark, S., & Lewandowsky, S. (2025). Seeing is believing: The continued influence of known AI-generated 'deepfake' videos. https://doi.org/10.21203/rs.3.rs-6471307/v1

Davis, M., & Fors, P. (2020). Towards a typology of intentionally inaccurate representations of reality in media content. *In* (pp. 291-304). https://doi.org/10.1007/978-3-030-62803-1_23

Dil, K., et al. (2024). Inability to detect deepfakes: Deepfake detection training improves detection accuracy but increases emotional distress and reduces self-efficacy. *Preprint*. https://doi.org/10.31219/osf.io/muwnj

Dolhansky, B., Howes, R., Pflaum, B., Baram, N., & Ferrer, C. C. (2019). The Deepfake Detection Challenge Dataset. *arXiv preprint arXiv:2006.07397*. https://arxiv.org/abs/2006.07397

Guess, A., Nagler, J., & Tucker, J. (2020). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances, 5*(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586

Hafiz, M. (2024). The era of artificial intelligence: Examining Indonesia's adaptability and legal challenges. https://doi.org/10.31219/osf.io/vk7jq

Harris, S., Hadi, H. J., Ahmad, N., & Alshara, M. A. (2024). Fake news detection revisited: An extensive review of theoretical frameworks, dataset assessments, model constraints, and forward-looking research agendas. *Technologies*. https://doi.org/10.3390/technologies12110222

Hägle, O., Escher, S., Heil, R., & Jahnel, J. (2024). Structuring different manifestations of misinformation for better policy development using a decision tree-based approach. *Policy & Internet, 17*(2). https://doi.org/10.1002/poi3.420

Hoek, S., Metselaar, S., Ploem, M., & Bak, M. (2024). Promising for patients or deeply disturbing? The ethical and legal aspects of deepfake therapy. *Journal of Medical Ethics*. https://doi.org/10.1136/jme-2024-109985

Iqbal, A., Shahzad, K., Khan, S. A., & Chaudhry, M. S. (2023). The relationship of artificial intelligence (AI) with fake news detection (FND): a systematic literature review. Global Knowledge, Memory and Communication. https://doi.org/10.1108/GKMC-07-2023-0264

Januário, T. (2025). Artificial intelligence and sexual offences: An analysis of deepfake pornography in light of criminal law. *Teisė, 134*, 48-60. https://doi.org/10.15388/teise.2025.134.4

Khimi, W., Albarqi, K., Saif, K., & Elhag, S. (2024). A systematic review on deep fake image generation, detection techniques, ethical implications, and overcoming challenges. *IJCI, 3*(8), 37-80. https://doi.org/10.59992/ijci.2024.v3n8p3

Kiliç, A., & Kahraman, Y. (2023). Current usage areas of deepfake applications with artificial

intelligence technology. *International E-Journal of Advances in Social Sciences*. https://doi.org/10.59534/jcss.1358318

LaVay, C., Jönsson, J., & Huzzard, T. (2020). Quantified control in healthcare work: Suggestions for future research. *Financial Accountability and Management, 36*(4), 461-478. https://doi.org/10.1111/faam.12242

Li, M., & Wan, Y. (2023). Norms or fun? The influence of ethical concerns and perceived enjoyment on the regulation of deepfake information. *Internet Research, 33*(5), 1750-1773. https://doi.org/10.1108/intr-07-2022-0561

Masud, U., Sadiq, M., Masood, S., Ahmad, M., & Abd El-Latif, A. A. (2023). LW-DeepFakeNet: a lightweight time distributed CNN-LSTM network for real-time DeepFake video detection. *Signal, Image and Video Processing*. https://doi.org/10.1007/s11760-023-02633-9

McCosker, A. (2022). Making sense of deepfakes: Socializing AI and building data literacy on GitHub and YouTube. *New Media & Society, 26*(5), 2786-2803. https://doi.org/10.1177/14614448221093943

Mendelsohn, B. (1965). Victimology: The victim and his criminal. *Columbia University Press.*

Nag, B. (2024). The evolution of ethical standards and guidelines in AI. In *[Book/Conference]* (pp. 45-84). https://doi.org/10.4018/979-8-3693-9173-0.ch003

Nait-Ali, A., Ridouani, M., Salahdine, F., & Kaabouch, N. (2023). Deepfake attacks: Generation, detection, datasets, challenges, and research directions. *Computers, 12*(10), 216. https://doi.org/10.3390/computers12100216

Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. N., & Nahavandi, S. (2022). Deep learning for deepfakes creation and detection: A survey. *Computers & Security, 114*, 102592. https://doi.org/10.1016/j.cviu.2022.103525

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital Society, 1*(2). https://doi.org/10.1007/s44206-022-00010-6

Pew Research Center. (2023). Public trust in elections and the impact of misinformation. https://www.pewresearch.org/politics/2023/05/15/public-trust-in-elections-and-the-impact-of-misinformation/

Putra, G., & Multazam, M. (2024). Law enforcement against deepfake porn AI. *EJCBLT, 1*(9), 58-77. https://doi.org/10.61796/ejcblt.v1i9.1015

Qureshi, J. and Khan, S. (2024). Deciphering deception – the impact of ai deepfakes on human cognition and emotion.. https://doi.org/10.20944/preprints202402.0135.v1

Rancourt-Raymond, A., & Smaïli, N. (2022). The unethical use of deepfakes. *Journal of Financial Crime, 30*(4), 1066-1077. https://doi.org/10.1108/jfc-04-2022-0090

Ruiter, A. (2021). The distinct wrong of deepfakes. *Philosophy & Technology, 34*(4), 1311-1332. https://doi.org/10.1007/s13347-021-00459-2

Ruvalcaba, Y., & Eaton, A. A. (2020). Nonconsensual porn as a form of technology-facilitated sexual violence: Understanding victims' experiences. *Violence Against Women, 26*(13–14), 1716–1735. https://doi.org/10.1177/1077801220935185

Ryu, B. (2024). Legal measures to improve protection for victims of deepfake sexual crimes. Korean Assoc Victimology, 32(3), 29-56. https://doi.org/10.36220/kjv.2024.32.3.29

Saxena, A., & Grewal, H. (2024). The use of deep fakes in social engineering attacks. In *[Book Title]* (pp. 293-306). https://doi.org/10.4018/979-8-3693-6665-3.ch013

Sensity AI. (2022). The state of deepfakes 2022 report. https://sensity.ai/reports/

Sharma, I., Jain, K., Behl, A., Baabdullah, A., Giannakis, M., & Dwivedi, Y. (2023). Examining the motivations of sharing political deepfake videos: The role of political brand hate and moral consciousness. *Internet Research, 33*(5), 1727-1749. https://doi.org/10.1108/intr-07-2022-0563

Harris, S., Hadi, H. J., Ahmad, N., & Alshara, M. A. (2024). Fake news detection revisited: An extensive review of theoretical frameworks, dataset assessments, model constraints, and forward-looking research agendas. *Technologies*. https://doi.org/10.3390/technologies12110222

Ternovski, J., Kalla, J., & Aronow, P. (2022). Negative consequences of informing voters about

deepfakes: Evidence from two survey experiments. *Journal of Online Trust and Safety, 1*(2). https://doi.org/10.54501/jots.v1i2.28

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Mor

Tuysuz, M. and Kılıç, A. (2023). Analyzing the legal and ethical considerations of deepfake technology. ISSLP, 2(2), 4-10. https://doi.org/10.61838/kman.isslp.2.2.2

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1). https://doi.org/10.1177/2056305120903408

Veljković, S., Ćurčić, M., & Gavrilović, I. (2024). Dark sides of deepfake technology. *Vojnotehnički Glasnik, 72*(3), 1441-1463. https://doi.org/10.5937/vojtehg72-49630

Venkateswarulu, S., & Srinagesh, A. (2024). Deepexplain: Enhancing deepfake detection through transparent and explainable AI model. *Informatica, 48*(8). https://doi.org/10.31449/inf.v48i8.5792

Von Hentig, H. (1948). The criminal and his victim. *Yale University Press*

West, S. M., Whittaker, M., & Crawford, K. (2020). Discriminating systems: Gender, race and power in AI. *AI Now Institute*. https://ainowinstitute.org/discriminatingsystems.pdf

Yadlin-Segal, A., & Oppenheim, Y. (2020). Whose dystopia is it anyway? Deepfakes and social media regulation. *Convergence: The International Journal of Research into New Media Technologies, 27*(1), 36-51. https://doi.org/10.1177/1354856520923963