Deepfakes in Iranian Private Law: An Analytical Exploration of Legal, Technical, and Social Challenges

Ali Farhani Panah
PhD Student of Private Law, University of Judicial Sciences and Administrative Sciences, Tehran, Iran

ABSTRACT

Deepfake technology, utilizing artificial intelligence to produce highly realistic yet fabricated multimedia content, presents a significant challenge to Iran's private law framework, particularly in addressing civil liability. This study highlights a critical knowledge gap in Iranian legal systems where the Civil Liability Act of 1960 struggles to address the complexities of proving fault and quantifying non material damages caused by anonymous and transnational deepfake distribution. The main research question is: How can Iran's private law regulate civil liability for deepfakes to balance technological advancement with the protection of individual rights? The aim is to propose a comprehensive regulatory framework by analyzing Iran's legal shortcomings through a qualitative and comparative methodology, drawing on international models like the European Union's AI Act and China's mandatory labeling regulations. The novelty lies in integrating Islamic jurisprudential principles, such as La Zarar (the prohibition of actions that result in damage or injury to others), Itlaf (Wasting) and Tasbib (Causation), to reform legal approaches, alongside advocating for detection technologies and media literacy. The findings highlight a pressing need for customized legal reforms to address the intricate legal, technological, and societal challenges posed by deepfakes in Iran. Without targeted measures, the risks of unchecked deepfake proliferation threaten to undermine individual rights and public trust.

Keywords Deepfakes, Civil Liability, Artificial Intelligence, Iranian Private Law

1. *INTRODUCTION*

Emerging technologies, particularly artificial intelligence (AI) and its applications such as deepfakes, have transformed the digital landscape, creating opportunities and challenges for legal systems including that of Iran, with unprecedented challenges. The virtual space, characterized by its virtual, electronic, and borderless nature, introduces unique attributes that impact traditional legal concepts, especially civil liability. These attributes encompass virtuality, user anonymity, the vastness and rapidity of information dissemination, and the complexity of control and governance [1].

Within this context, deepfake technology, which leverages artificial intelligence to generate deceptive yet realistic audio and visual content, poses significant threats to individual rights including privacy, reputation, and intellectual property. These threats are Aggravated by the inherent features of the virtual space, as those who create fake content often hide behind fake or anonymous identities, and this content spreads like wildfire across online platforms, it becomes really tough for legal systems to figure out who's responsible and how to compensate for the harm caused. As a result, exploring civil liability for deepfakes under Iran's private law calls for a fresh take on traditional legal ideas and a rethink of current laws to find a balance between encouraging new technology and protecting people's rights. The advent of deepfake technology, which employs artificial intelligence, notably Generative Adversarial Networks (GANs), to produce counterfeit multimedia content that appears authentic, has introduced unparalleled challenges across social, political, and legal spheres. This technology, derived from the terms "deep learning" and "fake," is capable of creating images, videos, and audio that are challenging for the average observer to discern from reality [2].

Deepfakes might open up some exciting possibilities in entertainment, but their darker side—like stealing identities, producing non-consensual explicit material, or spreading false information—poses serious risks to people's rights and the stability of society. [3]. Notable instances include the fabricated videos of Barack Obama in 2018 and Volodymyr Zelensky in 2022, which underscore the technology's capacity to manipulate public perception and instigate political turmoil [2].

These global threats have underscored the imperative for legal regulation of deepfakes, compelling legislators to seek balance between harnessing their advantages and mitigating their misuses [4]. In Iran, where cultural and social norms place a premium on privacy and dignity, The effects of this technology could be especially significant, especially given the widespread accessibility of deepfake creation tools, which have democratized their production beyond specialized entities [5].

Legally, deepfakes provoke critical inquiries concerning civil liability, intellectual property rights, and personality rights [6]. Nonetheless, Iran's legal system still hasn't developed a clear framework to confront this new phenomenon. The Civil Liability Act of 1960, while establishing a foundation for compensation, struggles with challenges such as establishing fault and quantifying damages arising within the complexities of this technology. International research indicates that jurisdictions like the European Union have embraced preemptive strategies through the AI Act of 2024 [7],

whereas Iran needs to reform its legal framework to protect individuals against digital exploitation. This study aims to examine the phenomenon of deepfakes through the lens of Iranian private law, particularly in terms of civil liability, and to offer recommendations for adapting the legal framework to meet this modern challenge. The primary question this study seeks to address is how civil liability arising from deepfakes can be regulated in Iran in a manner that balances technological innovation with the protection of individual rights. To this end, a qualitative and comparative analytical approach is employed. The research begins with a conceptual and legal analysis of deepfakes, with particular emphasis on Iranian law, especially the 1960 Civil Liability Act, which forms the foundation of compensation mechanisms in private law [6]. This analysis is further enriched by an examination of legal texts and interpretive practices to identify key shortcomings, such as the difficulty of establishing fault and the inadequacy of existing legal frameworks in addressing digital technologies. Thereafter, a comparative perspective is adopted, focusing on cutting edge legal systems, including the European Union (AI Act 2024), China (Cyberspace Administration Regulations 2023), and the United States (federal legislative proposals), to extract insights that may inform legal reform in Iran [7, 8].

This comparative analysis is grounded in reputable scholarly literature, including the works of Gupta (2023) and Kugler and Pace (2021), which critically examine the global challenges presented by deepfakes [2, 3]. The data gathered from academic literature, legal instruments, and international reports are analyzed inductively to uncover relevant legal paradigms and practical recommendations. By combining an internal critique of Iranian law with a comparative assessment of foreign legal systems, this approach enables the development of tailored solutions that align with Iran's cultural values while addressing the technical complexities of deepfake technologies [5].

The limitations of this study include the lack of domestic empirical data on deepfakes in Iran, a gap that is addressed through theoretical exploration and comparative analysis. Despite this constraint, the research provides a comprehensive and actionable assessment that not only clarifies existing legal gaps but also offers practical recommendations for reforming Iran's civil liability framework.

2. The Nature and Role of Deepfakes

As deepfake technology gains prominence across global discourse, understanding its foundational mechanisms becomes essential for grasping its legal and societal implications. This requires not only an exploration of the algorithms and techniques that drive deepfake creation, but also a careful assessment of how such technology interacts with broader legal concepts—especially within the context of Iranian private law. Therefore, before addressing the applications and impacts of deepfakes in various domains, it is imperative to first establish a clear and comprehensive understanding of their technical foundations and definitional parameters

2.1. Definition and Technology of Deepfakes

Deepfake technology, a term derived from the amalgamation of "deep learning" and "fake," represents one of the most advanced achievements of artificial intelligence in the realm of multimedia content creation, garnering significant global attention in recent years. At the core of this innovation lie advanced machine learning techniques, especially Generative Adversarial Networks (GANs) and Autoencoders, which are employed to generate manipulated images, videos, and voices that closely mimic real-life features and behaviors. According to the definition proposed in the European Union's AI Act amendment, a deepfake refers to "manipulated or synthetic audio, image, or video content" that "deceptively conveys a sense of authenticity or credibility, depicting individuals as saying or doing something they never said or did," generated through AI-based techniques [9].

This definition not only underscores the deceptive nature of deepfakes but also provides a legal framework for their identification and regulation, highlighting the importance of understanding this phenomenon in both

technical and social dimensions. Historically, the term “deepfake” was coined by a Reddit user who employed face-swapping technology to superimpose celebrities’ faces onto pornographic videos [10].

What distinguished this act was the simplicity and accessibility of open-source tools, which democratized the ability to produce such content. This development raised profound questions about authenticity, the perception of reality, and ethical implications, sparking widespread discourse across various domains. From a technical perspective, deepfakes are primarily generated through two main methods: Generative Adversarial Networks (GANs) and Autoencoders. In the GAN approach, two neural networks operate competitively: the Generator creates counterfeit content, while the Discriminator attempts to identify its falsity. This process continues until the Discriminator can no longer distinguish between fake and authentic content. In other words, the Generator acts as the “forger” and the Discriminator as the “detective,” ultimately reaching an equilibrium where the fabricated content becomes virtually indistinguishable [11,12].

Conversely, Autoencoders compress input data into a latent vector (encoding) and then reconstruct it (decoding), particularly for face-swapping, to produce manipulated content. Given the technical complexity of this technology, a precise understanding is essential for legal and ethical analysis. GANs, introduced by Ian Goodfellow and colleagues in 2014, create a zero-sum game between the Generator and Discriminator, yielding increasingly realistic content [13]. These networks, trained on large datasets, identify hidden patterns and utilize them to generate novel content. In the context of deepfakes, this may include human faces that never existed or videos that convincingly mimic an individual’s movements and speech [14].

Autoencoders, a type of artificial neural network, enable data reconstruction or alteration by learning compressed representations. In deepfake applications, they are typically used for face-swapping, overlaying one person’s face onto another’s body while preserving natural movements and expressions [15].

Despite their technical differences, both methods produce content that is challenging for humans and even detection algorithms to identify as fake. Beyond these primary methods, other technologies contribute to deepfake production. For instance, Natural Language Processing (NLP) techniques are employed to generate synthetic voices or alter speech. Tools like Lyrebird enable the creation of fake audio from typed text, which can be misused to forge vocal identities [9]. Additionally, deep learning algorithms are used to produce textual content, such as articles or social media posts, potentially leading to disinformation or author impersonation. This diversity in utilized technologies underscores the breadth and complexity of the deepfake phenomenon, emphasizing the need for multifaceted management approaches. Complementary technologies have also advanced deepfake development. For example, 3D rendering and motion capture techniques enhance the realism of fabricated videos by enabling precise replication of body movements and facial expressions, commonly used in gaming and filmmaking industries [15].

Algorithms like DeepFaceLab combine Autoencoders and 3D models for face-swapping, delivering high-quality results that can deceive even experts. Moreover, advancements in Convolutional Neural Networks (CNNs), which serve as a foundation for image and video processing, have improved the accuracy and speed of deepfake production [15]. However, these technologies are not without limitations. A primary challenge is the requirement for large, high-quality datasets to train models. Insufficient or non-diverse data can result in flawed outputs, such as facial distortions or inconsistent movements [14]. Additionally, the high computational resource demand, particularly for graphics processing units (GPUs), makes deepfake creation challenging for casual users, though open-source tools like FakeApp have partially alleviated this barrier [10].

Concurrently, efforts to detect deepfakes are progressing. Deep learning-based algorithms, such as advanced detection networks, can identify subtle cues like lighting inconsistencies or unnatural pixel patterns. This competition between deepfake creation and detection has evolved into an arms race within the AI domain. Emerging trends indicate further expansion of this technology. For instance, advanced generative models like StyleGAN enable the creation of images and videos with unprecedented detail [16]. Additionally, integrating deepfakes with augmented reality (AR) and virtual reality (VR) technologies could produce entirely new multimedia experiences, further blurring the line between reality and fabrication.

These advancements, coupled with increased access to deepfake tools, heighten the urgency of addressing the technical and regulatory aspects of this phenomenon. A critical aspect of defining deepfakes is distinguishing them from other forms of media manipulation. While media forgery has a long history—from manipulated photographs in the 19th century to edited videos in contemporary times—deepfakes, due to their reliance on AI and ability to generate wholly synthetic content, introduce an unprecedented level of deception. For example, in 1840, Hippolyte Bayard created the first known fake photograph depicting a staged suicide [9].

In contrast, deepfakes can produce entirely fabricated videos of real individuals saying or doing things they never did, profoundly obscuring the boundary between reality and forgery and engendering unique legal and ethical challenges.

Consequently, the legal definition of deepfakes is of paramount importance. As noted, the proposed amendment to the EU AI Act offers a comprehensive definition focusing on their deceptive nature and impact on individuals, which could serve as a model for other legal systems, including Iran's. However, Iran currently lacks a specific legal definition for deepfakes, which may complicate the identification and prosecution of misuse cases. For instance, in cases involving identity theft or the dissemination of unethical content, the absence of a legal definition can hinder the process of proving offenses. Thus, formulating a precise and comprehensive legal definition for deepfakes within Iranian law is a critical step toward managing this phenomenon. Ultimately, deepfake technology is not merely an advanced technical tool but a social and legal phenomenon necessitating interdisciplinary examination. A deep understanding of its technical mechanisms, including GANs, Autoencoders, and complementary technologies like CNNs and 3D modeling, is vital for analyzing its legal and ethical ramifications. By creating seemingly authentic content, this technology challenges traditional notions of authenticity and forgery, compelling legal systems to reconsider foundational concepts such as liability, ownership, and personality rights. Subsequent sections will explore the applications and impacts of this technology on society and Iran's legal framework.

2.2. Applications and Impacts of Deepfakes

Deepfake technology, renowned for its ability to create fabricated yet highly realistic multimedia content, exerts extensive and multifaceted impacts across various facets of life, including education, entertainment, medicine, politics, and economics. While this technology offers significant opportunities for innovation, it also poses serious ethical, legal, and social challenges. This section explores the positive and negative applications of deepfakes and their broader implications. In the realm of education, deepfakes can facilitate interactive and visually engaging learning experiences by simulating historical or scientific figures. For instance, students could engage in dialogues with digital representations of past luminaries, thereby gaining a deeper understanding of complex concepts. In Iran, where the educational system often relies on traditional methods, this technology could enhance learning motivation, provided robust technical infrastructure and rigorous content accuracy oversight are in place. In the entertainment industry, deepfakes reduce production costs and enable the recreation of scenes or characters, fostering creative opportunities. In Iranian cinema, this technology could elevate the quality of productions and enhance global competitiveness, contingent upon adherence to intellectual property rights. Additionally, deepfakes have innovative applications in medicine; for example, by reconstructing the voices of patients with debilitating conditions such as ALS, they enable communication and improve quality of life.

Nevertheless, the threats posed by deepfake technology are far from negligible. One of the most pressing concerns relates to its use in the creation of pornographic content, an application that not only constitutes a significant portion of deepfake misuse globally but also stands in stark opposition to the cultural, religious, and moral values underpinning Iranian society. Such content has the potential to inflict profound social and psychological harm, particularly upon the individuals depicted without their consent. Accordingly, Iran's legal framework necessitates the development of robust regulatory mechanisms to prevent and penalize such misuse effectively.

In the political domain, deepfakes present acute risks by enabling the fabrication of statements or actions attributed to public officials and political figures. These manipulations can distort public discourse, erode trust in political institutions, and foment unrest during sensitive periods, such as electoral campaigns.

The economic implications are similarly alarming: with the increasing digitization of Iran's banking and financial systems, the use of synthetic audio or video to facilitate fraud or identity theft poses a substantial and evolving threat. This situation calls for urgent reinforcement of cybersecurity infrastructure and the integration of deepfake detection protocols into financial regulatory frameworks.

From a social perspective, the misuse of deepfakes could undermine national cohesion by provoking ethnic, sectarian, or ideological tensions.

At the same time, it is important to acknowledge the technology's potential for positive use, such as in educational initiatives aimed at increasing public literacy regarding media manipulation and digital misinformation.

Perhaps most critically deepfakes challenge the integrity of Iran's legal and judicial systems by casting doubt on the reliability of audiovisual evidence. In the absence of advanced forensic tools and proper judicial training, the risk of erroneous verdicts based on manipulated content becomes a serious concern. the

emergence of deepfakes necessitates a reevaluation of evidentiary standards and the incorporation of AI literacy into legal practice.

In sum, while deepfake technology offers certain opportunities, its potentially disruptive impact on Iran's legal, political, and cultural institutions demands a carefully calibrated response. Legal and policy interventions must be informed by Iran's unique normative framework and social sensitivities, ensuring that innovation does not come at the cost of justice, security, or societal integrity.

3. Comparative Analysis of International Approaches to Regulating Deepfakes

This section undertakes a comparative analysis of international regulatory approaches to managing this phenomenon, focusing on models such as mandatory labeling in China and the European Union's AI Act. It extracts practical lessons for Iran's legal system, evaluating the strengths and weaknesses of each approach while proposing analytical and precise solutions for regulating deepfakes, tailored to Iran's legal and cultural framework.

3.1. United States: Balancing Freedom and Responsibility Under Limited Oversight

The regulation of deepfakes in the United States is guided by caution and adaptability in consideration of the First Amendment protection of free speech. The Department of Defense is required by the 2020 National Defense Authorization Act to detect deepfake threats, while legislation pending in 2023, deepfakes Accountability Act of 2023, would make labeling and criminalizing harmful content mandatory [4]. However, proving malicious intent or direct harm remains challenging due to the technical complexities of deepfakes [19]. This challenge is apparent in "false light" tort claims that seek redress for reputational harm but are often unsuccessful because they must prove malice[16, 17].

As opposed to centralized regulation, America's approach draws on individual responsibility and responsive intervention, eschewing sweeping preemptive regulation. Though flexibility protects innovation, it increases the possibility of abuse, especially when deceiving content goes viral and finding its sources is difficult.

Iran can take from this lesson in its judicial system the need for striking a balance between free expression and protection of individual rights. Establishing particular tort actions for reputational harm similar to "false light" would prove an efficient instrument provided that definitive requirements for proving harm are set in order to minimize evidentiary complications. The practice, especially in a culturally diverse society in Iran, would safeguard victims of deepfakes without precipitating extensive censoring.

3.2. China: Centralized Oversight and Mandatory Transparency as Control Mechanisms

China adopts a centralized and stringent approach through its "Regulations on the Management of Internet Information Services with Deep Synthesis" (2022), mandating the labeling of deepfakes and prohibiting their use to spread false news [4]. These laws make technology developers responsible for adherence, and violations are punishable through detention [4]. The 2023 "Interim Regulations on the Management of Generative AI Services" show relative flexibility as well by striking a balance between control and innovation [8].

This system based on mandatory disclosure and platform accountability has partially contained the dissemination of false content, albeit through limiting individual freedoms and necessitating strong infrastructure from the state.

The model has an advantage in quickly detecting harmful content and reducing social harm, providing an example for countries that have centralized systems.

Iran can draw on China's commitment to disclosures and accountability. Requiring labeling of deepfakes on Iran specific platforms such as Aparat or Namasha would increase disclosures and avoid unwitting dissemination of false content. The approach is possible due to Iran's current regulatory bandwidth and must be applied carefully not to inhibit innovation.

3.3. *European Union: Risk-Based Transparency and Investment in Detection*

The European Union pursues a comprehensive, risk based approach through the AI Act (2024). it regulates deepfakes as deceptive content. This law mandates developers to adhere to transparency and safety standards and emphasizes the use of advanced detection tools [7]. The definition within this framework emphasizes the deceptive nature of deepfakes, and regulation is tuned in proportion to the risk level of content. Implementation is hindered by high compliance costs and technical constraints [9].

Through a blend of technology and openness, EU policymaking attempts to balance protection and innovation while relying on sophisticated infrastructure and global cooperation for its success. As opposed to China's system of centralized control, risks are managed through EU prevention and prioritizing corrective behavior over punishment. Iran can take from its approach an appreciation for investing in detection technology and having risk-based policies in place. Creating indigenous tools for detecting deepfakes in cooperation with universities and knowledge-based industries would enable the infrastructure for swift

identification of false content. With Iran's technical limitations, this lesson requires long-term planning and resource budgeting.

3.4. Singapore: Limitations of Oversight Based on General Laws

Singapore regulates deepfakes under the Protection from Online Falsehoods and Manipulation Act (POFMA, 2019), which allows for the removal or correction of fake content. However, its reliance on general laws and the difficulty of proving malicious intent limit its effectiveness, rendering it reactive rather than preventive [4].

Without specialized tools such as labeling or sophisticated detection, this method emphasizes the shortcomings of current laws in responding to the nuances of deepfakes.

Singapore's structure compares unfavorably with China and the EU in that it has lower preventive capability and is susceptible to the swift transmission of online content. Singapore is an example demonstrating that dependency on general laws, as Iran has in its 2009 Computer Crimes Act, is inadequate for guiding deepfakes. Iran needs to create special and particular legislation that surpasses current systems in order to respond to the nuances of the technology. The lesson reinforces the requirement for current laws to be modified.

3.5. India: Sectoral Oversight and the Need for Industry Collaboration

India shares its cultural and infrastructural context with Iran but does not have distinct deepfake laws and must fall back on overall cybercrime legislation. Nevertheless, attempts at limiting its use in entertainment have been made [18].

The case of a fabricated video involving Rashmika Mandanna highlights the social and legal harms of deepfakes in developing societies [18].

India's model in its infancy stages emphasizes cooperation with certain sectors such as entertainment and media, short of having comprehensive regulation. Though showing the possibility of targeted regulation, the model showcases the shortcoming of not having wider regulation mechanisms. Iran can learn from India the need to collaborate with certain sectors, for instance, entertainment and online media. Cooperation with institutions of culture such as the Ministry for Culture and Islamic Guidance in formulating targeted regulation in these areas may prove an applicable measure for reducing harm from deepfakes on increasingly local platforms.

4. Deepfakes within the Framework of Iran's Current Laws

Deepfake technology, which utilizes artificial intelligence to produce fabricated yet highly realistic audio and visual content, has presented Iran's legal system with unprecedented challenges. This technology not only threatens individual privacy and reputation but also undermines public trust in media and judicial evidence. This section first analyzes Iran's existing laws, including the Civil Liability Act of 1960, the Computer Crimes Act of 2009, and the Authors' Rights Protection Act of 1969, in terms of their compatibility with this emerging phenomenon. Subsequently, it examines the shortcomings and challenges of these laws in addressing deepfakes, elucidating why the current legal framework is ill-equipped to counter this digital threat.

4.1. Analysis of Existing Laws

In Iran's legal system, the Civil Liability Act of 1960 serves as the cornerstone for compensating damages in private law but faces significant limitations when confronting challenges posed by cyberspace and emerging technologies like deepfakes [1].

Designed for tangible and traditional settings, this law proves inadequate in addressing the complexities of the cyber environment, characterized by virtuality, user anonymity, and the rapid dissemination of information. Particularly in deepfake cases, where fabricated content is generated using artificial intelligence and disseminated on digital platforms, establishing the elements of civil liability, such as causation and harmful acts, encounters substantial obstacles [1].

For instance, identifying the perpetrator and verifying the link between their actions and the resulting harm is exceedingly difficult for Iran's judicial system due to the virtual and anonymous nature of this space. This underscores that the Civil Liability Act of 1960, grounded in fault and proof of causation in the physical world, requires revision and adaptation to address digital phenomena like deepfakes. A fundamental challenge in pursuing civil liability in cyberspace is the difficulty of proving fault and identifying the offender.

This issue becomes particularly acute in deepfake related cases, as creators of fabricated content often employ advanced tools such as encryption, virtual private networks (VPNs), and fake identities, rendering their tracking and identification highly challenging and, in some instances, practically impossible for Iran's judicial system [1]. Moreover, the transnational and elusive nature of cyberspace, where data and activities

swiftly transcend geographical borders, severely limits the ability to enforce legal sovereignty and pursue effective prosecution. This situation not only highlights the weaknesses of current legal mechanisms but also emphasizes their inadequacy in addressing emerging digital abuses, particularly in the realm of complex technologies like deepfakes.

The lack of sufficient technical and legal tools to adapt to these challenges further underscores the urgent need to revise existing laws. To formulate effective regulations for deepfakes, the media function of cyberspace and the foundational principles of freedom of expression must be seriously considered. Cyberspace and digital platforms, as conduits for the free flow of information, play a pivotal role in safeguarding freedom of expression. Consequently, any legal intervention must be designed with precision and care to avoid undermining these core values. One proposed solution is the mandatory labeling of AI-generated content, including deepfakes, which could enhance transparency in the digital environment without leading to widespread censorship or unnecessary restrictions.

This approach not only enables users to distinguish fake content from authentic material but also establishes a reasonable balance between protecting individual rights and preserving freedom of expression. Furthermore, strengthening international cooperation and developing technical tools to trace the origins of fake content could assist the legal system in addressing the transnational challenges posed by deepfakes. These measures, combined with domestic legal reforms, can lay the foundation for effectively confronting emerging technologies.

Iran's legal system relies on traditional and existing laws to address deepfakes, each of which, despite potential capacities, is severely limited due to its age and lack of alignment with the complexities of this technology. The Civil Liability Act of 1960, as the primary basis for damage compensation in private law, defines liability in Article 1 based on fault and causation [6].

This framework is effective in traditional cases, such as physical or material damages, but when addressing deepfakes, which are often produced by anonymous or transnational actors, proving fault becomes a significant obstacle. For instance, if a fabricated video depicts an individual in a false and embarrassing situation, the victim must identify the creator to seek compensation, a task rendered practically impossible due to the use of tools like VPNs and anonymous platforms [2].

Moreover, Article 8 of the Civil Liability Act, which addresses non material damages, lacks clear criteria for assessing harms such as damage to reputation or psychological distress caused by deepfakes.

Research indicates that visually deceptive content can have profound emotional impacts on individuals [21], yet the absence of judicial precedent in Iran for quantifying such damages renders the law ineffective in practice. This inefficiency is particularly pronounced in cases where deepfakes, with their strong visual impact, create false memories or psychological stress, a phenomenon that has also raised concerns in judicial interrogations [19].

The Computer Crimes Act of 2009, enacted to regulate digital offenses, criminalizes the dissemination of false or distorted content under Articles 16 and 17. In theory, these provisions could cover deepfakes published with the intent to defame or mislead, but the lack of explicit reference to advanced technologies like deepfakes limits their protective scope [19].

For example, Article 16 focuses on criminalizing obscene or immoral content, but applying it to a deepfake produced solely to deceive public opinion (e.g., forging a public official's speech) is challenging [18]. This gap, compared to countries like China, which have enacted specific regulations for fake content [4], highlights Iran's lag in updating cyber laws. Additionally, the law emphasizes identifying the perpetrator, an impractical requirement given the transnational and anonymous nature of deepfakes.

From the perspective of personality rights, implicitly derived from civil and Islamic legal principles in Iran, deepfakes could be considered a violation of privacy. However, the absence of a clear definition of "digital identity" as part of these rights renders legal protection incomplete. For instance, the case of Rashmika Mandanna's fabricated video in India, which left victims defenseless against digital identity violations, could similarly cause irreparable harm in Iran without a specific legal framework.

The Authors' Rights Protection Act of 1969, designed to safeguard literary and artistic works, is ill-equipped to address digital abuses stemming from deepfakes. This law recognizes the material and moral rights of creators but focuses on traditional works like books and music, neglecting modern technologies such as the digital forgery of an artist's face or voice. For example, if a deepfake reconstructs a singer's voice to produce an unauthorized work, the violation of their moral rights is evident, yet the law provides no specific tools to pursue such violations [18].

In Iran's rapidly growing digital entertainment industry, this gap leaves artists vulnerable to digital exploitation. In Iran's legal system, the Civil Liability Act of 1960 is recognized as the cornerstone of damage compensation in private law.

However, this law reveals its inefficiencies when confronting challenges posed by emerging technologies, particularly deepfakes. Deepfakes, generated using artificial intelligence and advanced techniques, are often created by anonymous or transnational actors, causing significant damages, particularly of a non-material nature.

The law, rooted in the establishment of fault, faces serious obstacles in these cases, as identifying the perpetrator and proving their intent or negligence is often practically impossible. Furthermore, the Civil Liability Act lacks clear criteria and mechanisms for compensating non-material damages, such as harm to reputation, privacy violations, or psychological injuries caused by fake content. These shortcomings are particularly critical as the need to protect individuals from such damages is increasingly felt in the digital era.

In contrast, the Islamic jurisprudential principle of La Zarar (No Harm), rooted in the Prophetic tradition "There shall be no harm or reciprocating harm" (La Zarar wa La Zirar) and verses such as Surah Baqarah 2:231, offers a different approach. This principle, which holds a significant place in Islamic jurisprudence, emphasizes the negation of any harm and the necessity of its compensation, even when fault cannot be explicitly proven.

Unlike the Civil Liability Act of 1960, which ties compensation to the establishment of fault, the La Zarar principle provides a broader perspective and can serve as a basis for compensating non material damages. In deepfake cases, this principle can serve as a basis for holding producers of fake content liable, as they indirectly harm individuals' reputation and rights through the creation and dissemination of such content. Thus, reforming existing laws to encompass damages caused by deepfakes, grounded in the La Zarar principle, can facilitate compensation for non material harms not fully addressed in the Civil Liability Act of 1960. In comparison, more advanced legal systems, such as that of the United States, utilize intellectual property claims to protect artists from digital forgery [19].

In Iran, however, the absence of judicial precedent and updated definitions leaves this domain devoid of effective protection. Although these three laws were effective in their time, they appear inadequate in addressing the unique characteristics of deepfakes, such as rapid production, difficulty of detection, and widespread dissemination, and require fundamental revision.

4.2. Shortcomings and Challenges

The shortcomings of Iran's current laws in addressing deepfakes, which utilize artificial intelligence to produce fabricated yet highly realistic audio and visual content, extend beyond legal structure to encompass operational, technical, and social challenges that exacerbate this inefficiency.

This technology, by threatening individual privacy, reputation, and public trust in media and judicial evidence, places Iran's legal system in a precarious position.

The following sections comprehensively examine these challenges. One of the most significant barriers in deepfake related cases is the difficulty of proving fault and identifying the perpetrator. Both the Civil Liability Act of 1960 and the Computer Crimes Act of 2009 rely on identifying the wrongdoer and establishing their intent or negligence, but deepfake technology renders this requirement a dead end. Content creators often operate outside Iran's judicial jurisdiction, using tools such as encryption, VPNs, foreign servers, and fake identities, making their tracking virtually impossible [6, 17].

For instance, if a fabricated video depicts an individual in a false and humiliating situation, the victim must identify the creator to seek compensation, a task fraught with significant obstacles due to the transnational and anonymous nature of deepfakes [2]. This issue is equally evident in criminal proceedings, where video evidence, once considered conclusive, has lost credibility due to the potential for digital forgery. If a defendant claims that a video presented against them is a deepfake, judges without advanced detection tools cannot verify its authenticity, reinforcing the principle of "doubt in favor of the accused" to the advantage of wrongdoers [17].

Furthermore, assessing non material damages, such as emotional harm or reputational damage caused by identity forgery, is complicated by the absence of clear judicial criteria, leaving judges in ambiguity [21]. The lack of advanced detection tools severely limits the capacity of Iran's judicial institutions and digital platforms to counter deepfakes. Unlike the European Union, which promotes investment in detection technologies like Media Forensics through the AI Act of 2024 [9], Iran lacks the technical infrastructure necessary for rapid identification of fake content.

This weakness not only complicates legal prosecution but also renders domestic digital platforms, such as Aparat, vulnerable to the widespread dissemination of deepfakes. For example, fake content may be accepted

as evidence in criminal cases, while detecting its inauthenticity without advanced technology is impossible [20]. This limitation undermines trust in video evidence within the judicial system and heightens the risk of deepfake misuse.

Iran, due to infrastructural constraints and limited investment in artificial intelligence, lags behind countries like the United States, which benefit from advanced detection tools [9]. Insufficient training of judges and judicial experts in emerging technologies further widens the gap between digital realities and legal frameworks. Detecting deepfakes requires technical expertise that is currently scarce in Iran's judicial system [20].

Research indicates that a lack of technical expertise among judicial decision makers can exacerbate deepfake threats [9], a problem more pronounced in Iran due to limited educational resources. The absence of ongoing training programs for judges on digital technologies restricts their ability to handle deepfake related cases, transforming this inefficiency into a systemic challenge. From a social perspective, deepfakes pose a serious threat to public trust in media and cultural cohesion in Iran. In a society with heightened religious and cultural sensitivities, the dissemination of fake content, such as a video depicting an individual committing an immoral act, could trigger severe social reactions, ethnic tensions, or even instability [5].

This risk is amplified by the lack of sufficient media literacy among Iranian users, who struggle to distinguish fake content from authentic material and are easily swayed [19]. A comparison with India, where the fabricated video of Rashmika Mandanna had widespread social repercussions [21], suggests that Iran is similarly vulnerable. For instance, a comparable deepfake in Iran could have even more devastating effects due to cultural and religious sensitivities, yet the current legal system lacks the tools for swift and effective response [21].

The transnational activities of deepfake producers turn legal prosecution into a doubly daunting challenge. Iran lacks effective international agreements to track and prosecute individuals producing fake content abroad [4]. This limitation, compared to countries like China, which have strengthened international cooperation to regulate digital content [4], further highlights Iran's inefficiencies. The global nature of deepfakes necessitates cross-border coordination, but sanctions and political constraints diminish Iran's capacity to participate in such efforts. These challenges, from the structural inefficiencies of laws in proving fault and compensating non material damages to the lack of advanced detection tools, judicial expertise shortages, social threats, and transnational limitations, underscore the urgent need for a comprehensive overhaul of Iran's legal approach to deepfakes.

Existing laws not only fail to protect victims but are also ineffective in preventing the proliferation of deepfakes. This inefficiency erodes public trust in the legal system and media, making structural reforms, investment in detection technologies, and enhanced media literacy increasingly imperative. The phenomenon of deepfakes, due to their complex technical nature and the often anonymous identity of producers, poses significant challenges to establishing civil liability in Iran's legal system. The Civil Liability Act of 1960, which centers on proving fault (intent or negligence) as a prerequisite for compensation, operates inefficiently against this emerging technology.

The first obstacle is the difficulty of identifying the deepfake producer, as such content is often disseminated through foreign platforms or anonymizing tools. Moreover, proving that the producer acted with intent to harm or through negligence is practically impossible due to technical complexities and the lack of direct evidence. These challenges are intensified in cases involving non-material damages, such as harm to reputation or privacy violations, as the existing law provides no clear criteria for establishing fault in such instances. In this context, the Islamic jurisprudential principle of Tasbib (causation), which emphasizes establishing a causal link between a harmful act and the resulting damage, offers an effective solution to overcome these challenges. According to this principle, civil liability is established when causation between an individual's act and the resulting harm is verified, even if fault is not explicitly proven.

Unlike the fault centric approach of the Civil Liability Act of 1960, Tasbib prioritizes examining the cause and effect relationship. In deepfake cases, this approach could leverage detection technologies, such as analyzing deepfake algorithms or tracing the source of dissemination, to establish causation. For instance, if it is determined that fake content originated from a specific source and caused harm, Tasbib could serve as the basis for liability without requiring proof of the producer's intent or negligence.

However, Iran's current legal system has not fully utilized the potential of the Tasbib principle. The lack of legal and technical mechanisms for tracking and analyzing deepfake content complicates the establishment of causation.

Additionally, the Civil Liability Act of 1960 lacks provisions specifically addressing issues arising from emerging technologies, limiting judges' ability to rely on jurisprudential principles like Tasbib. In contrast,

more advanced legal systems, such as the European Union, have developed regulations to identify and trace fake content, facilitating the establishment of causation [2].

This experience suggests that integrating Tasbib with technical tools could provide an effective framework for addressing deepfakes. Thus, the challenges of proving fault in deepfake cases highlight the need to revise the approach of the Civil Liability Act of 1960. The Tasbib principle, with its emphasis on causation over fault, can serve as a foundation for developing new laws. This transformation requires establishing technical mechanisms for tracking fake content and enacting regulations to facilitate the establishment of causation in technology driven cases. Such an approach is not only consistent with jurisprudential foundations but also responsive to the legal needs of society in the digital era.

4.3. Proposals and Solutions

To address the growing challenges posed by deepfakes in Iran, the development of a comprehensive and multidimensional regulatory framework is essential, integrating legal reform, advancement of detection technologies, public education, and international cooperation. This framework must not only counter the threats of fabricated content but also promote responsible innovation. The following sections analytically detail each component, addressing implementation challenges and proposing viable solutions.

4.3.1. Legal Reform

The initial step in addressing the challenges posed by deepfakes is to reform existing legal frameworks and establish a strong legal basis for regulating this emerging technology. A foundational element of these reforms should be the introduction of a clear, legally binding definition of “harmful deepfakes,” distinguishing content that violates privacy, damages reputations, or threatens public safety from harmless or creative uses. This definition could be incorporated through amendments to the 2009 Computer Crimes Act or added to the regulatory scope of the Supreme Council of Cyberspace.

Introducing explicit legal prohibitions on the creation and distribution of deepfake content without consent, similar to China’s approach to harmful content [4], would serve as a strong deterrent. Furthermore, requiring written consent for the use of a person’s image or voice would reinforce the concept of digital identity as an extension of personality rights, thereby enhancing legal protections for victims [19].

The United States “false light” tort doctrine, which outlines specific standards for compensating reputational damage, could serve as a model for revising Iran’s 1960 Civil Liability Act to encompass non-material harms [17]. Additionally, requiring the labeling of AI generated content, as stipulated in the European Union’s AI Act, would improve transparency on digital platforms and help users better distinguish between authentic and synthetic content [7].

However, several challenges must be addressed in implementing these legal reforms. First, the technical complexity of deepfake technologies may hinder legislative action due to lawmakers’ limited understanding. Second, overly broad or vague definitions risk enabling censorship and may conflict with the principles of free expression. Third, enforcing labeling requirements on smaller or foreign digital platforms would be costly and require a robust regulatory infrastructure, which is currently underdeveloped in Iran.

To navigate these obstacles, the creation of interdisciplinary task forces comprising legal scholars and technology experts is recommended. These teams could develop precise and contextually suitable definitions. To mitigate censorship risks, the regulations should narrowly target "harmful" content with clear criteria rather than all AI generated material. To address implementation costs, authorities could offer incentives such as tax exemptions for compliant platforms and impose heavy penalties on violators. Starting with domestic platforms like Aparat or Namasha as pilot projects could also help manage logistical and financial burdens.

These proposed legal reforms align with international standards, including the EU’s AI Act and U.S. tort law, and are also grounded in Islamic jurisprudence, particularly the principles of La Zarar (no harm), Itlaf (waste) [1], and Tasbib (causation) [2]. These principles offer a comprehensive framework for assessing harm and assigning liability, forming a moral and legal foundation for the suggested regulations. Defining “harmful deepfakes” and requiring the labeling of AI-generated content not only promote transparency and protect rights but also reflect the jurisprudential focus of Tasbib and Itlaf on causality and the obligation to compensate both material and nonmaterial damages, including reputational harm.

Deepfakes represent a novel legal challenge that conventional liability systems may not adequately address. The measures proposed here including updating laws, creating targeted regulations, and utilizing deepfake

[1] The rule of wasting is one of the most important rules by which issues related to liability (ḍamān) and civil liability in Islamic jurisprudence (fiqh) and law are resolved.

[2] The rule of Tasbib (intercession, causation) is one of the jurisprudential rules of law regarding guarantee, which in civil law, compensation and in criminal law, punishment.

detection technologies are consistent with the principles of La Zarar, Itlaf, and Tasbib. These Islamic legal doctrines support a comprehensive approach to harm and compensation, offering a culturally and legally appropriate framework for regulating new technologies. Under the principle of Tasbib, any individual who directly or indirectly causes harm to another's property, rights, or life is liable for compensation. This principle can be applied to deepfake creators, who cause reputational and personal harm through the creation and dissemination of false content. Reforming existing laws based on Tasbib and La Zarar would enable victims to seek redress for nonmaterial harms that are not adequately covered under current statutes like the 1960 Civil Liability Act. Notably, Tasbib Principle emphasizes establishing causation between a harmful act and the resulting damage, without deeming fault a prerequisite. This Principle supports the establishment of deepfake laws by ensuring compensation for victims through civil remedies and punishment for perpetrators through criminal sanctions. Civil laws provide financial and injunctive relief for harms like defamation and emotional distress, while criminal laws deter malicious acts like fraud, election interference, and non consensual porn.

The rule of Itlaf is also applicable, as deepfakes can "waste" intangible assets such as reputation, dignity, and financial stability through the spread of false or defamatory content. For instance, a deepfake depicting someone in a scandalous or criminal scenario can irreparably damage their social and professional life, constituting a harm under Itlaf. Civil laws grounded in this principle could recognize such harms as actionable torts like defamation or emotional distress, making platforms or individuals legally accountable. Remedies could include monetary compensation or content removal, thereby integrating Islamic principles into modern legal enforcement.

This framework is particularly effective in deepfake cases, where proving intentional wrongdoing is often difficult. Establishing clear regulatory measures such as labeling suspicious content and developing mechanisms to trace its origin would support the application of Tasbib, Itlaf, and La Zarar in proving harm and establishing liability. In parallel, deploying deepfake detection technologies could help verify the authenticity of content and identify perpetrators. Together, these proposals offer a legal model that is both rooted in Islamic jurisprudence and equipped to meet the demands of the digital era. By focusing on causation and compensation, this model provides a comprehensive response to the unique threats posed by deepfake technology.

4.3.2. Development of Detection Technologies

The second pillar of this framework is investing in the development of deepfake detection technologies to enhance the ability of judicial institutions, digital platforms, and ordinary users to identify fake content. These technologies include advanced video analysis tools and blockchain for verifying content authenticity. Collaboration with reputable domestic universities, such as Sharif University of Technology and the University of Tehran, and knowledge based companies (danesh bonyan) could facilitate the localization of these technologies, reducing reliance on foreign solutions.

Blockchain, by recording content metadata in an immutable database, not only verifies video authenticity but also traces the origin of forgeries.

Establishing a specialized unit under the supervision of Iran's Cyber Police (FATA) or the Ministry of Communications could centralize these efforts and improve inter-agency coordination. Developing these technologies faces significant hurdles.

First, the high cost of research, development, and implementation, particularly under economic sanctions, poses a serious challenge. Second, a shortage of skilled professionals in artificial intelligence and blockchain in Iran could slow progress. Third, there is a risk of misuse of these technologies for unauthorized surveillance or privacy violations, necessitating careful oversight. To manage costs, leveraging joint public private funding and utilizing global open-source tools are recommended to reduce expenses and accelerate access to technology.

To address the shortage of specialists, expanding short term training programs and university collaborations is advised. To prevent misuse, developing transparent regulatory frameworks and mandating privacy compliance in the design of these tools are essential. Additionally, implementing pilot projects on a small scale, such as on domestic platforms like Aparat, could serve as an initial step to control costs and evaluate the effectiveness of these technologies.

4.3.3. Public Education and International Cooperation

The third pillar of this framework is enhancing public awareness and strengthening international cooperation, both critical for reducing societal vulnerability to deepfakes. Boosting media literacy through educational campaigns led by the Islamic Republic of Iran Broadcasting (IRIB), the Ministry of Education, and the Ministry of Culture and Islamic Guidance can empower citizens to more effectively identify fake content.

These programs should be simple, engaging, and culturally tailored; for instance, using short animations or interactive games could facilitate learning across age groups.

Additionally, international cooperation with countries like China and the European Union, which have advanced regulations and technologies for managing deepfakes, could enhance Iran's technical expertise [7,8].

However, emphasis must be placed on localizing these technologies and supporting domestic knowledge based companies to avoid excessive reliance on foreign solutions.

Sporadic educational campaigns often have short term impacts and are forgotten after completion. International cooperation is complicated by sanctions and political considerations, potentially limiting access to advanced technologies. Furthermore, insufficient funding for widespread educational programs could hinder achieving this goal. To enhance effectiveness, educational programs should be continuous and mandatory, particularly in schools targeting younger generations. Using educational games and interactive content could increase engagement and retention. In terms of international cooperation, focusing on knowledge exchange with regional countries, rather than dependence on the West, and supporting domestic startups could circumvent sanctions and make collaboration more cost effective and sustainable.

Allocating specific government budgets and attracting private investment could also secure the necessary resources for these programs. This proposed framework, integrating legal reforms, technical advancements, and social awareness, could position Iran as a regional leader in managing deepfakes.

Successful implementation requires long term commitment, targeted investment, and precise coordination among government institutions, the private sector, and civil society to protect individual rights while promoting responsible innovation. Given the rapid pace of technological advancements, these measures must be designed dynamically and flexibly to remain adaptable to future challenges.

5. Conclusion

The rapid proliferation of deepfake technology, driven by advancements in artificial intelligence, has ushered in a new era of legal, technical, and social challenges that profoundly test the resilience of Iran's private law framework. This study has argued that Iran's existing legal apparatus, particularly the Civil Liability Act of 1960, is ill equipped to address the complexities of civil liability arising from deepfakes, necessitating a transformative approach to safeguard individual rights while fostering responsible technological innovation.

The core contention is that a multidimensional regulatory framework, grounded in both modern legal reforms and Islamic jurisprudential principles, is essential to navigate the unprecedented threats posed by deepfakes in Iran's unique cultural and legal context.

The evidence marshaled throughout this analysis underscores the multifaceted nature of the deepfake challenge. Legally, the Civil Liability Act's reliance on proving fault falters in the face of anonymous and transnational deepfake producers, rendering the identification of perpetrators and the compensation of nonmaterial damages, such as reputational harm or psychological distress, nearly impossible.

Comparative insights from global jurisdictions, such as the European Union's risk based AI Act and China's mandatory labeling regulations, reveal the value of proactive and transparent approaches that Iran could adapt to enhance accountability without stifling innovation.

Technically, the absence of advanced detection tools and judicial expertise exacerbates the vulnerability of Iran's legal system, undermining trust in multimedia evidence and complicating prosecution. Socially, deepfakes threaten cultural cohesion and public trust in a society where religious and ethical sensitivities amplify the impact of fabricated content, as evidenced by parallels with cases like the Rashmika Mandanna incident in India.

This article's conceptual innovation lies in its integration of Islamic jurisprudential principles, notably La Zarar (No Harm), Itlaf (wasting or destruction of another's property) and Tasbib (Causation), to reframe civil liability for deepfakes. By prioritizing harm compensation and causal linkages over fault-based requirements, these principles offer a culturally resonant foundation for legal reform that aligns with Iran's jurisprudential heritage.

This approach not only addresses the limitations of the current fault centric framework but also provides a flexible paradigm for tackling emerging digital threats.

Furthermore, the proposed solutions, encompassing legal amendments to define harmful deepfakes, investment in indigenous detection technologies, and public education campaigns to bolster media literacy, reflect a holistic strategy that balances prevention, enforcement, and societal resilience. Ultimately, the challenge of deepfakes in Iran transcends mere legal technicalities; it demands a reevaluation of how private law can adapt to the digital age while preserving core societal values.

This study advocates for a forward-looking framework that harmonizes technological progress with the protection of dignity, privacy, and trust. By drawing on global best practices and grounding reforms in Islamic principles, Iran has the opportunity to not only address the immediate threats of deepfakes but also position itself as a regional leader in managing the legal implications of artificial intelligence. The path forward requires sustained commitment to interdisciplinary collaboration, ensuring that legal, technical, and social strategies evolve in tandem to meet the demands of an increasingly complex digital landscape.

REFERENCES

[1] Malakouti, R. (2020). How to apply the Pillars of Civil Liability in the Cyberspace of Instagram. Communication Research, 27(101), 143-157. doi: 10.22082/cr.2020.116275.1943
[2] Gupta, S. (2023). Deepfakes and intellectual property: Emerging legal dilemmas. International Journal of Technology Law, vol. 12, no. 2, p. 132-155.
[3] Kugler, M. B., Pace, C. (2021). Deepfakes and the law: Privacy, publicity, and emotional harm. Stanford Law Review, vol. 73, no. 3, p. 620-666.
[4] Vinogradov, A., Kuznetsova, E. (2024). Global approaches to regulating deepfakes: A comparative analysis. Comparative Law Journal, vol. 19, no. 3, p. 217-237.
[5] Bosman, J., Smith, A., Taylor, R. (2021). Artificial intelligence and the rise of deepfakes: Technical and ethical challenges. Journal of Digital Ethics, vol. 5, no. 3, p. 260-263.
[6] Hossain, M. (2024). Civil liability in the digital age: Addressing deepfake harms. Asian Journal of Legal Studies, vol. 8, no. 4, p. 2267-2272.
[7] Demkin, V. (2024). Regulating AI in the European Union: A comparative legal perspective. European Law Review, vol. 49, no. 1, p. 73-87.
[8] Zhang, A. H. (2025). The promise and perils of China's regulation of artificial intelligence. Columbia Journal of Transnational Law, vol. 63, no. 1, p. 3-51.
[9] Herke, Csongor. (2023). Deepfake: blessing or curse? legal regulatory aspects. Pro Futuro: Jovo Nemzedekek Joga, 2023(1), 157-178.
[10] Smith, H., & Mansted, K. (2020). Weaponised Deep Fakes: National Security and Democracy. Australian Strategic Policy Institute, International Cyber Policy Centre.
[11] Kulkarni, Vaishnavi, & Sivaramachandran, Bhanusshre. (2024). Tackling the multifaceted legal dilemmas of deep fake technology. Jus Corpus Law Journal, 4(3), 217-230.
[12] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In Advances in Neural Information Processing Systems 27 (pp. 2672–2680).
[13] Tolosana, R., et al. (2020). Deepfakes and beyond: A survey of face manipulation. IEEE Access, p. 3-8.
[14] Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Nießner, M. (2016). Face2Face: Real-time face capture and reenactment of RGB videos. ACM Transactions on Graphics, 35(4), Article 41, 1–14.
[15] Karras, T., et al. (2019). A style-based generator architecture for generative adversarial networks. IEEE Conference on Computer Vision and Pattern Recognition, p. 7-10.
[16] Vyas, Anoo Dinesh. (2024). United states of deepfake. Tennessee Law Review, 92(1), 307-354.
[17] Mullen, Molly. (2022). new reality: deepfake technology and the world around us. Mitchell Hamline Law Review, 48(1), 210-234.
[18] Tiwari, R. (2024). Deepfakes in the entertainment industry: Opportunities and legal challenges. Media and Law Review, vol. 15, no. 15(1), 42-48.
[19] Healy, J. (2025). Deepfakes and the law: Addressing the legal challenges of AI-generated content. Journal of Technology and Law, 12(3), 518-553.
[20] Interesse, G. (2022, December 20). China to regulate deep synthesis (deepfake) technology starting 2023. *China Briefing*. https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/
[21] Kugler, M. B., & Preminger, L. (2024). *Deepfakes in entertainment: Redefining publicity rights*. Harvard Journal of Entertainment Law, 45(2), 828-833.