Proceedings of ICSPHS 2026 Symposium:Ethics, Law, and Psychology: Interdisciplinary Reconstruction of Humanities in Medicine
DOI: 10.54254/2753-7048/2026.ZJU31599

Criminal Law Determination of the Abuse of Deepfake Technology

Tianxiao Ma

School of Law, University of Nottingham, Nottingham, United Kingdom
matianxiao1@outlook.com

Abstract. In recent years, deepfake technology has been widely used in the generation and replacement of information such as images, audio and video due to its high fidelity, low threshold and easy dissemination. However, the abuse of this technology may pose serious threats to individual rights, social order, and national security. At present, the legal regulations in China regarding deepfake technology are still not perfect. There are problems such as inconsistent standards of identification, low deterrent power of punishment, a fragmented legal system, and difficulties in evidence determination. By comparing the regulatory experiences of regions like the EU, the UK, and the US, it is found that they have different focuses in risk prevention and industry self-discipline, which provide useful references for China. Therefore, by learning from international experience and combining with China's actual national conditions, this paper proposes that China should make more efforts in improving legislation, increasing punishment provisions, and stipulating the responsibilities and obligations of platforms or service providers, and build a more systematic and effective legal regulation system to deal with the multiple challenges brought by deepfake technology, and promote the coordinated development of technology governance and legal liability.

Keywords: Deepfake, legal regulation, artificial intelligence, criminal risk

1. Introduction

In recent years, artificial intelligence has developed rapidly. Through the use of artificial intelligence, "deepfake" technology has emerged, enabling the generation and replacement of information such as images, audio, videos, and virtual scenes with extremely high authenticity [1]. From entertainment, art to education and business, deepfake has brought people an unprecedented immersive experience and creative expression space, greatly enriching the content and forms of digital life. However, the "double-edged sword" nature of technology is particularly prominent in this field. With the gradual lowering of the usage threshold of deepfake technology and the popularity of open-source tools, the abuse of deepfake has posed unprecedented severe challenges to individual rights, social stability, and national security.

Specifically, deepfake technology can generate extremely realistic images, voices, and even dynamic behaviors. This makes it highly vulnerable to malicious use. For instance, at the level of infringing on personal rights, this technology could be used to create false indecent videos, carry out

DOI: 10.54254/2753-7048/2026.ZJU31599

defamation or extortion [2]. Criminals carry out telecommunications fraud by imitating the voices and appearances of public figures or their relatives; they even forge the statements of political figures, businesspeople, etc., to disrupt the financial market or interfere with elections [2]. For society, fabricated videos of disaster scenes, terrorist incidents or official statements may spread rapidly on the internet, causing public panic and undermining the foundation of social trust. In terms of national security, deepfake technology may be used to create diplomatic tensions, fabricate military developments, and incite social division, becoming a new tool for information warfare and manipulation of public perception [2]. These abuses of deepfake technology not only seriously infringe upon citizens' dignity, privacy rights, portrait rights and property security, but also may affect social consensus, threaten political security and national stability. Due to the ease of production, rapid dissemination and difficulty in identification of the products generated by deepfake technology, there are gaps in the legislative field, and the evidence collection is somewhat difficult, making it impossible to effectively control it. Therefore, the governance of this field is extremely urgent.

At present, the legal regulatory system for deepfake in the country is not yet complete, and there are some legal loopholes. Firstly, there is a lack of unified legislation, resulting in the absence of a unified judgment standard and different sentencing results in different regions for the same case. Secondly, the criminal penalty threshold of the criminal law is relatively high, and some cases of deepfake that do not cause serious consequences to have not been punished, leading to a low cost of committing crimes. Thirdly, some legal fields and departmental functions overlap, and conflicts may occur during the judgment process. Finally, due to the concealment and other characteristics of emerging technologies, the cost and difficulty of evidence collection have greatly increased. Therefore, this study analyzes the criminal risks of the abuse of deepfake technology and the inadequacies of the existing legal policies and discovers the existing legal problems. At the same time, by comparing the relevant laws of Artificial Intelligence (AI) deepfake in China and abroad, and by drawing on international experience, feasible suggestions for improving and perfecting the legal system in China are proposed to build a more comprehensive and effective legal system.

2. Analysis of criminal risks arising from the abuse of deepfake technology

2.1. Definition and application areas of deep faking technology

"Deepfake risk" refers to the internal competition between the 'generator' and 'discriminator' neural models in the generative adversarial network. The generated videos, images, sounds, and scenes, etc., due to their high transmissibility, may pose threats to individuals, society, and the country [3].

Deepfake technology is mainly applied in the fields of images and audio. In image generation, deep synthesis technology can create or replace high-definition and highly realistic videos. Audio-video synthesis is the most typical representative of deepfake technology, which is known as the "AI face and voice substitution" technology. Audio deep synthesis technology can be applied in scenarios such as music generation, voice assistants, and audio books [4].

2.2. Reasons for the abuse of deepfake technology

Firstly, deepfake technology usually operates through open-source algorithms and user-friendly software, so even ordinary people can easily master it and generate highly realistic fake content [3]. Secondly, there is already plenty of open-source software, online platforms and cheap apps available. Moreover, the generated content can be widely disseminated in a short period of time

DOI: 10.54254/2753-7048/2026.ZJU31599

through platforms such as short-video apps. This results in the low cost of infringing upon and violating the rights of "deepfake" false information [5]. Furthermore, AI systems can automatically delete operational traces and are highly covert. Moreover, the electronic network can employ technologies such as virtual IP to enhance its covert nature, making it extremely difficult to trace and obtain evidence [6].

2.3. Analysis of criminal risks associated with deepfake technology

The abuse of deepfake technology infringes upon individuals' basic rights, including infringements on the rights of portrait, reputation, privacy and property. It also undermines public safety and social trust mechanisms, such as creating social panic, inciting mass incidents, and disrupting financial order through the use of deepfake technology. This includes political security (such as interfering with elections), military security (disseminating false information), and ideology, etc.

For individuals, on some websites in the country, the sale of pornographic videos featuring celebrities has made many women victims of the abuse of "deepfake" technology [7]. For society, during the period when the country was fully combating the COVID-19 pandemic, if someone used "deepfake" technology to create a false video in which an authoritative expert claimed that "the epidemic is impossible to prevent and control", it would very likely cause instability throughout the entire society [7]. For countries, the behaviors or statements of some political figures generated through "deep forgery" technology led to internal unrest in the country. For example, the official Twitter account of The Associated Press was stolen, and its false news such as "Obama is injured" caused almost all the US economic market to plunge [1].

3. The current situation and challenges of criminal legal regulations on deepfake-related issues in the country

3.1. Analysis of criminal law legal regulation

According to Article 2, Paragraph 1 of the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Defamation and Other Related Crimes through the Use of Information Networks" promulgated on September 6, 2013, in general circumstances, if a video generated through deepfake technology is viewed more than 5,000 times or forwarded more than 500 times, it meets the sentencing criteria of "serious circumstances" stipulated in the Criminal Law [8]. For example, Article 246 of the Criminal Law stipulates that those who openly insult others or make up facts to slander others, thus causing serious circumstances, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights. However, unlike the actual number of times that network users browse and forward content, the automatic clicks and forwards by the algorithm make the videos and other content generated by the application's deepfake technology extremely likely to meet the "serious circumstances" element in criminal law for sentencing. Regarding the automatic clicks and browsing by the algorithm, there are two issues. Firstly, due to the protective legal status and the principle of restraint of criminal law, the criminal law cannot be overly proactive when responding to the abuse of "deepfake" technology [8]. Secondly, under the influence of algorithm automation, once deepfake content is released, it is very likely to reach the criminal sentencing standards. This results in the negligible effect of non-criminal regulations on deepfake technology [2]. Overall, the current criminal sentencing standards do not fully take into account the particularity of artificial

DOI: 10.54254/2753-7048/2026.ZJU31599

intelligence algorithms and the rapid dissemination characteristics of deepfake content, so they cannot be fully applicable.

In addition, it may meet multiple charges in a case. Zheng Gaojian showed in his research that if criminals use synthetic works to perpetrate fraud, they may have illegal and criminal behaviors such as violating citizens' personal information and producing improper deepfake content, then it is still unclear whether they should be punished for multiple crimes together or the most serious crimes should be punished [9].

3.2. Difficulties faced by the current legal system

Firstly, due to the lack of a clear and unified legal standard for cases involving "deepfake" technology, different judicial authorities in different regions may encounter the situation where they make different judgments for similar AI deepfake cases [9].

Secondly, the criminal law adheres to the principle of restraint, stipulating that the criminal liability standard will only be met when the social harm reaches a certain level. Therefore, a large number of deepfake behaviors, although their actions inherently carry extremely high potential risks, have not been punished because they did not cause serious consequences [10].

In addition, cases related to deepfakes may involve multiple aspects such as administrative violations and criminal offenses [5]. There may be gaps or overlapping areas between different regulations. However, which department and which law should be the main basis for law enforcement may lead to disputes.

Moreover, the concealment of AI generation technology includes automatically clearing operation logs, forging access records, and covering up the real track through virtual IP, device fingerprint camouflage and other technologies [6]. It brings special challenges to the collection, examination and identification of criminal evidence. And electronic data, as the main evidence for recording behavioral trails, has the characteristics of being prone to tampering and being easily lost.

4. International experience and comparison of legal regulation of deepfakes

4.1. Analysis of the EU "artificial intelligence act" and UK-related artificial intelligence laws

The various safeguard measures introduced by the EU against deepfake technology include transparency obligations (the "Artificial Intelligence Act"), prevention of algorithm amplification and reduction of risks by digital platforms (the "Digital Services Act"), and sanctions for particularly widely disseminated unauthorized pornographic content without consent (the "Directive on Combating Violence against Women and Domestic Violence"). In Article 3, Paragraph 60 of the "Artificial Intelligence Act", the EU clearly defined deepfake as "deepfake" referring to the use of artificial intelligence technology to generate or manipulate audio content that is difficult for viewers to distinguish as real or fake, involving persons, places, or events, etc. Additionally, it classified the areas of application of artificial intelligence into different risk levels and implemented different regulatory intensities for each risk category. Moreover, it specifically stipulated obligations and responsibilities for this field through the act [11]. For example, Article 5 of the AI Act lists the industries where the use of artificial intelligence is strictly prohibited. By definition, this means that there are unacceptable risks associated with the application of artificial intelligence in these industries. This includes government conducting social scoring, real-time remote biometric identification in public places (except for authorized law enforcement agencies), and so on [12]. And Article 6 and Annex III specify the high-risk application areas of artificial intelligence, covering

DOI: 10.54254/2753-7048/2026.ZJU31599

eight fields including critical infrastructure, education, employment, law enforcement, judiciary, welfare, immigration, and democratic procedures. The artificial intelligence systems classified as high-risk must fulfill numerous obligations when in use. For instance, Article 9 stipulates the establishment of a risk management system, Article 13 requires it to be transparent, Article 14 ensures human supervision, and Article 15 requires it to have high levels of robustness, accuracy, and cybersecurity, etc. Finally, in Article 52, low-risk artificial intelligence systems are defined as those generating or replacing images, sounds, etc., and interacting with users, etc. Low-risk artificial intelligence systems need to fulfill the obligation of transparency, and users have the right to know their operation information [12].

The UK government released the white paper "AI Regulatory Approaches to Support Innovation" in March 2023, but it is not legally binding. That is, the UK has not made explicit legislation in the field of artificial intelligence; instead, it has proposed five key principles: safety, security and robustness, appropriate transparency and explainability, fairness, accountability and governance, as well as the ability to challenge and provide remedies, aiming to strike a balance between the innovation of artificial intelligence technology and necessary guarantees [13].

4.2. Comparison of deepfake laws and regulations in the EU and the UK

The EU AI Act divides the development of AI systems into different risk categories. For application areas where unacceptable risks are involved, such as facial recognition, risks will not be allowed to exist. The act also clearly stipulates the conditions for developing these "high-risk" artificial intelligence systems. Other permitted categories are limited-risk applications and extremely low-risk applications [14]. However, unlike the AI risk management policies of the European Union, the effectiveness and ethical legitimacy of the UK's artificial intelligence governance measures carry risks. These risks are particularly high for general artificial intelligence systems that affect multiple fields [15]. The UK believes that when regulating the AI sector, the impact of regulatory actions on the development of the sector needs to be considered. In the "Artificial Intelligence White Paper" released by the UK in March 2023, the flexibility of UK AI control was determined. This moderate flexibility approach contrasts sharply with the approach of the EU. Some civil society organizations believe that the EU's approach is too rigid and cannot provide adequate and lasting protection [15].

5. Feasibility proposal

5.1. Improving legislation and judicial interpretations

For legislation, it is necessary to clearly incorporate biometric information such as facial features, voiceprints, gait, and behavioral habits into the special protection category of personal information, and to establish a hierarchical protection system in the crime of infringing upon citizens' personal information under the Criminal Law based on the type of information and its corresponding importance [16]. Because biometric information is unique, permanent and unchangeable, once it is leaked or misused, it will cause profound and irreversible damage to personal identity security, property security and even social order [17]. Therefore, legislation should distinguish it from ordinary personal information, set stricter standards for its acquisition, storage, use and processing, and make corresponding adjustments in criminal penalties, setting differentiated sentencing grades based on the sensitivity and harmful consequences of the information.

Furthermore, by gradually improving judicial interpretations and strengthening case guidance, the quantitative threshold for "deepfake"-related crimes can be moderately lowered to enhance the legal

DOI: 10.54254/2753-7048/2026.ZJU31599

deterrent effect. Additionally, it is necessary to clearly define the special identification criteria for "deepfake" crimes, such as considering factors like the actual degree of harm and the cost of debunking rumors when determining the sentence [16].

5.2. Improving the penalty regulations

Introduce punitive damages to deter the offenders who abuse deepfake technology. Due to the extremely low cost of infringement and violation in creating "deepfake" false information, the responsibility-bearing system for dealing with false digital information in the country is unable to effectively curb the implementation of the abuse of "deepfake" technology. There is not enough criminal and illegal cost for such behaviors, and the deterrent effect is insufficient. Therefore, it is necessary to introduce a highly punitive civil liability to improve this situation. The punitive damages system can meet this requirement [5].

5.3. Clearly defining the division of responsibilities and obligations

When the abuse of deepfake technology leads to infringement, the responsible parties should be classified as the users and disseminators of the technology, the client, the technology provider and the dissemination platform. The users and disseminators, as the direct infringers, should bear the main responsibility, while the client should bear joint liability. As the technology provider, if one still provides technical support when knowing that the other party is abusing deepfake technology, they should bear the legal responsibility for assisting infringement, such as constituting the serious circumstances may constitute the crime of assisting information network crime activities stipulated in Article 287, Paragraph 2 of the Criminal Law. Finally, for the dissemination platform, based on the original 2009 "Infringement Liability Law", which is still followed in the "Infringement Liability Chapter" of the "Civil Code", the "Safe Harbor Principle" and "Red Flag Principle" established by the law, the platform has the obligation to promptly block the dissemination of infringement and illegal content [4]. When the infringement of the video is of a serious nature, the party involved also needs to bear joint liability.

In addition, the obligations of service providers and platforms need to be clarified in Chinese legal policies, that is, the data retention obligations of platforms, as well as the information retention of users. This is to reduce the difficulty of evidence tracing.

5.4. Tiered classification system supervision

China may be able to learn from the EU in classifying the risks of AI application fields and prohibiting the application of this technology in some extremely dangerous areas, such as those that affect national and social security and stability, including controlling public cognition by manipulating the subconscious [12]. In high-risk areas, efforts should be made to strictly control the risks and minimize them. For instance, in the EU's artificial intelligence act, it mentions the high-risk applications of artificial intelligence in eight fields. China may be able to draw on their approach and classify these eight core areas as high-risk levels. For other low-risk areas, people can learn from the United States and the United Kingdom, which rely on legal obligations of platforms or service providers and industry self-regulation. This way, people can avoid the application risks of deepfake technology to a certain extent while not hindering the innovation and development of technology as much as possible.

DOI: 10.54254/2753-7048/2026.ZJU31599

6. Conclusion

In conclusion, while deepfake technology brings convenience and enjoyment to people, it also brings many harms to individuals, society, and the country. Currently, there are several problems in China's criminal law, such as the lack of unified legislative provisions, inconsistent judgment standards, difficulties in evidence certification, high punishment thresholds, and insufficient punishment intensity. Therefore, by drawing on international experience and combining with China's actual national conditions, in terms of legal system improvement, people can achieve this through improving legislation and judicial interpretations, improving punishment regulations, clarifying the division of responsibilities and obligations, and adopting a classification supervision system. This will help address the numerous legal challenges brought about by deepfake technology.

As for whether multiple crimes should be punished concurrently or the most serious crime should be punished alone when a case of abuse of a certain deepfake technology involves multiple illegal acts, there is still no clear conclusion. Therefore, the operability of some of the legal suggestions in this study has certain limitations. Looking to the future, China should continuously monitor the development of deepfake technology and the emergence of new abuse behaviors, in order to promptly promote legislation to adapt to the rapid development of artificial intelligence technology. At the same time, international cooperation should be strengthened, and the integration of technological innovation and legal governance should be encouraged, developing traceable and verifiable digital identity and content authentication technologies to fundamentally curb the abuse of deepfake.

References

[1] Qi, W. (2025) The National Security Risks of Deepfake Technology and the Integrated Governance Approach. China Science and Technology Forum, (7), 105-115.
[2] Ting, Y. (2022) The Alienating Criminal Risks of Deepfake Technology and Their Regulation. Master's Thesis, Guizhou University.
[3] Guobin, Z. and Yifan, C. (2025) Conceptual Model and Generation Mechanism of Deepfake Risks from the Perspective of Public Security. Academic Monthly, 57(8), 82-94.
[4] Dongliang, L., An, H. and Xiaoke, Y. (2025) The Abuse of Deepfake Technology and Its Legal Regulation. Journal of Yanbian University (Social Sciences Edition), 58(1), 80-93.
[5] Yuanting, Z. (2022) Legal Regulation of Abuse of "Deep Fakes" in the Era of Artificial Intelligence. Theoretical Monthly, (9), 118-130.
[6] Ning, M. and Hui, Y. (2021) The Regulatory Challenges of Deepfake Technology and Its Legal Responses. Changbai Journal, (5), 94-101.
[7] Teng, L. (2020) Construction of Criminal Regulation System for "Deep Fakes" Technology. Zhongzhou Journal, (10), 53-62.
[8] Ying, J. (2021) The Dimensions and Limits of Criminal Regulation of "Deepfake" Technology in Artificial Intelligence. Nanjing Social Sciences, (9), 101-109.
[9] Gaojian, Z. (2025) The Criminal Response to the Abuse of Deepfake Technology. Legal Science (Journal of Northwest University of Political Science and Law), 43(3), 56-68.
[10] Ran, C. (2024) Legal Regulation of Deepfake Manipulation of Sexual Information. Law, (3), 76-90.
[11] Łabuz, M. (2025) A Teleological Interpretation of the Definition of DeepFakes in the EU Artificial Intelligence Act —A Purpose-Based Approach to Potential Problems With the Word "Existing". Policy and Internet, 17(1).
[12] Wörsdörfer, M. (2024) Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope? Global Business and Organizational Excellence, 43(3), 106-126.
[13] Krook, J., Winter, P., Downer, J. and Blockx, J. (2025) A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance. AI and Ethics, 5(4), 4069-4090.
[14] Xalabarder, R. (2025) Regulating AI: Differences Between the U.S. and the EU. The Columbia Journal of Law & the Arts, 48(3), 325.

DOI: 10.54254/2753-7048/2026.ZJU31599

[15] Roberts, H., Babuta, A., Morley, J., Thomas, C., Taddeo, M. and Floridi, L. (2023) Artificial intelligence regulation in the United Kingdom: A path to good governance and global leadership? Internet Policy Review, 12(2), 1-31.
[16] Haiyan, Z. and Longke, T. (2025) The Path Selection for Regulating AI "Deep Fakes" under Criminal Law. Legal Daily.
[17] Senlin, H. (2025) The Criminal Law Regulation of Personal Biometric Information and Deep Fakes in the Context of Digital Economy. Journal of Neijiang Normal University, 40(12), 93-101.