Academic Education Publishing House

Philosophy and Social Science Vol. 3 No. 5, 2026

The Impact of Deepfake on Personal Information Interests and Criminal Law Protection

Liu Xinyu

School of Political Science and Law, University of Jinan, Jinan, China

Abstract: As an emerging technology, deepfake is bound to bring new vitality to social development. However, its abuse has already exceeded the technical scope of artificial intelligence and gradually slid into the gray area of criminal activities. The irrational and improper use of this technology in social life has also brought many problems and challenges to criminal governance. Therefore, during its application, we must apply it rationally; otherwise, it is difficult to achieve its social benefits. Currently, there are practical difficulties in regulating deepfake technology in China. For example, whether the crime of infringing upon personal information should include the false personal information produced by deepfake, how to handle the regulatory mechanism for the frequent false infringement content in the online space, and how to achieve a balance between the technical neutrality and ethical norms in the current technology are all issues that we need to solve. To address these problems, we need to seek solutions from aspects such as legal systems, regulatory models, and upholding moral bottom lines.

Keywords: Deepfake; Personal Information Legal Interest; Ethical Norms; Criminal Law Protection

In recent years, artificial intelligence technology has developed rapidly, but it has also brought certain governance challenges to society. For instance, we may come across a private video of a public figure on the internet, and the person's appearance and voice can convince us beyond doubt of their true identity. However, later, a professional institution confirmed that every frame of the video was artificially synthesized and forged. Such incidents undoubtedly damage the reputation of the individuals involved and also expose new security issues regarding citizens' personal information. As early as December 2017, such cases occurred in the United States. User "Deepfakes" used synthesis technology to maliciously replace the face of a Hollywood actress, making her the main character in a pornographic video and uploading it to the "Reddit" website, pushing public opinion to a peak.This is where the term "deepfake" originated. To protect the personal information protection system, we need to use criminal law as the ultimate barrier for social defense. By conducting in-depth analysis of the technology of deepfake itself and the legal interests it infringes upon, we can propose the criminal law response strategies.

1. Analysis of Deep Faking Technology and Its Impact on Personal Information Legal Interests

1.1 The Theoretical Explanation and Feature Analysis of Deep Faking

The term "deep faking" is derived from the English words "deep learning" and "fake". Its core lies in the application of Generative Adversarial Network (GAN) and deep learning models.It is possible to generate highly realistic fake content at an extremely low cost. GAN achieves technological progress through an "adversarial" mechanism and a dynamic game mechanism between two sets of neural networks. In this model, the "generator" neural network builds a target image model based on the source data and is responsible for generating fake images or audio-visual content. The "discriminator" neural network, on the other hand, uses the real target image as a benchmark to test the authenticity of the generator's output. If the "discriminator" determines that the generator's output does not match the real target image, the result will be automatically returned to the "generator" for re-modification until it conforms to the target image. After multiple adversarial optimizations, ultimately, highly realistic audio-visual works can be synthesized.

The technical features of deepfake technology are as follows: The first aspect is high

authenticity. The traditional synthesis method requires technicians to extract the facial features of the target person frame by frame and manually match the light and shadow as well as the mouth shape. The generated content is monotonous and the modification traces are obvious, resulting in significant deviations between the algorithm-generated content and the real sample.The dynamic game mechanism of the generative adversarial network model is a form of "unsupervised learning", which can automatically optimize until it meets the target requirements under the instructions of the algorithm.The second aspect is ease of operation. In the "unsupervised learning" mode, the APP application can achieve the user's purpose with a one-click operation, reducing the operational difficulty, and the technology is no longer monopolized by the government and large companies, promoting the further development of this technology towards simplified operation. The third aspect is self-evolvability. Deepfake is a product of artificial intelligence. The algorithm has the characteristic of self-updating. Deepfake can upgrade and evolve by relying on the GAN model. In the adversarial mode, it gradually approaches the real target image. Its technological breakthrough speed far exceeds the expectations of society and the construction of defense systems. In response to the characteristics of deepfake, China currently has corresponding legal regulations to deal with it.

1.2 The Impact of Deep Fakes on Personal Information Legal Rights

Deepfake technology is widely applied in various fields. The illegal forms mainly involve illegal collection of biometric information, forging identities to carry out other criminal activities, and creating false information. Firstly, personal information and large-scale data are the sources of deepfake works. However, the problem of illegal data collection has become increasingly prominent nowadays, infringing upon the autonomy of personal information. These platforms obtain users' biometric data and other privacy information through covert means such as making users "silently" agree to lengthy terms of use or excessively expanding access to their mobile phone permissions. Taking the "ZAO" face-swapping APP as an example, this APP uses tactics in its user agreement terms, making users agree that the platform can have permanent usage rights to their uploaded facial data.This once again highlights the importance of protecting personal information. Additionally, other criminal activities carried out using deepfake technology pose more direct harm to citizens. For instance, criminals can combine AI face-swapping and voice cloning techniques to simulate specific identities and carry out targeted fraud. In 2023, in Zhejiang, fraudsters, with the aim of making profits, transformed citizens' photo portraits into 3D avatars to deceive new Alipay users and obtain corresponding red envelope rewards. Their actions constituted the crime of fraud.Finally, the deepfake technology poses a particularly serious threat to citizens' right to privacy regarding their portraits and reputations.The infringement of portrait rights manifests as follows: Firstly, using someone else's portrait rights without their permission; Secondly, creating false content through deepfake technology to defame, tarnish or damage someone's portrait rights. Unauthorized use of false content generated from personal biometric data directly violates Article 1019 of the Civil Code. At the same time, it has caused great damage to the privacy rights and reputation rights of the parties involved, leading to a transformation of the mode of infringement of privacy rights from invading private spaces to fabricating private activities.

Therefore, the technical characteristics and complexity of deepfake technology determine that it is necessary to regulate through criminal law means. As mentioned earlier, deepfake has already posed threats to personal information legal interests in terms of personality and property, involving multiple subjects and multiple legal interests. Moreover, in the context of the rapid spread of information networks, the infringement of legal interests by deepfake technology is irreversible, and for the victims of the fabricated pornographic videos, even if the videos are taken down and compensation measures such as apology are made, their reputation and privacy still suffer irreparable damage. In recent years, the number of crimes related to deepfake in China has gradually increased, and the cases have become increasingly complex. Data information has already become an important legal interest. In the face of these increasing risks, it is reasonable to expand the criminal charges to ensure a dynamic balance between technological innovation protection and criminal punishment within the criminal justice framework.

2. The Practical Challenges in Regulating Deepfake Crimes

The rapid development of deepfake technology has presented unprecedented challenges to the protection of personal information legal rights. Due to the rampant phenomenon of illegal collection and trading of citizens' personal information, it has also given rise to various illegal acts such as infringement of portrait rights, telecommunications fraud, and defamation and slander. This constitutes a complete criminal chain covering "data collection - intermediary transactions - illegal applications".At present, the criminal law's handling of deepfake technology follows a "heavy at both ends, light in the middle" approach.That is, the criminal law will regulate the behaviors of abusing citizens' personal information at the front end and the behaviors of using deepfake technology to create false information at the back end, thus forming a dual protection approach against the abuse of personal information by deepfake technology.

2.1 The Application Difficulties of the Current Normative System

The relevant laws on criminal law and personal information protection have significant lag in regulating deepfake behavior. Deepfake not only creates false information but also abuses personal biometric information. On one hand, the criminal law provisions regarding the crime of infringing upon citizens' personal information mainly target illegal acquisition, sale, or provision of "true" personal information. However, there is controversy over whether the "false personal information" generated by deepfake technology falls within the protection scope of this crime. The affirmative view holds that even if the forged information is associated with a real individual, it may still infringe upon the reputation, privacy, etc. of the real person, and such false information may be used for identity fraud, etc., thus deserving criminal protection. The opposing view believes that this crime protects "true" personal information, and the forged information is not real data and does not directly involve the rights and interests of the information subject. It may be more suitable to be regulated through insults, defamation, etc. Moreover, criminal law should maintain restraint. The governance of false information should primarily rely on civil tort liability or administrative supervision rather than directly applying criminal sanctions.On the other hand, the abuse of personal biometric information through deepfake technology can lead to various crimes such as defamation, fraud, and crimes against computer information systems. Moreover, the current laws lack specific charges for AI-generated false information and also fail to regulate the illegal use of biometric information after its legal acquisition.For instance, if an enterprise employee legally obtains facial data from the database but later uses deepfake technology for criminal activities, this situation leads to the fact that in judicial practice, traditional criminal charges are often relied upon for regulation, making it difficult to achieve precise punishment and prone to the occurrence of inconsistent judgments for the same case.

2.2 The Regulatory Standard System is Not Yet Mature.

When deepfake content becomes prevalent in the online space, the public's ability to judge the authenticity of information will weaken, and people will gradually become numb to the flood of false information. This is very likely to disrupt social order. And deepfake, whether in terms of data sources or the circulation of the fabricated works, cannot do without the control of regulatory entities. Regarding data source collection, the current regulatory mechanism centers on public authorities as the main regulatory entity. They still rely heavily on traditional information protection models, protecting only personal information as the sole protected object, such as ID cards, names, contact details, etc. However, for advanced biometric technologies like facial recognition, voice recognition, and fingerprint recognition, although there have been regulatory guidelines for deepfake technology, there are still problems with insufficient implementation. Moreover, although China has a relatively complete legal system for data collection, use, and sharing, there are still some ambiguous areas and implementation challenges, which also increase the difficulty of effective supervision by platforms. For the dissemination of deepfake products, it cannot be separated from the control of enterprise platforms. They can both cause a sharp increase in the number of products and control the harmful consequences at the bud stage. Therefore, special attention should be paid to the regulatory capabilities and responsibilities of enterprise platforms, especially in the review

process, where the standard of strength needs to be accurately grasped. If the platform conducts excessive reviews, it may mistakenly identify legal content as illegal forgery, affecting freedom of speech and creative enthusiasm. If the platform's review is too lax, it may lead to the large-scale inflow of infringing content into the market, damaging citizens' rights and interests. However, in reality, platforms often cannot achieve a good balance between the two and are difficult to prevent the infringement behaviors brought about by deepfake.

2.3 The Balance Between Technological Neutrality and Ethical Norms

Deepfake, as a technological tool, inherently possesses a "neutral" characteristic. It can be used in legitimate scenarios such as film production and classroom teaching. However, it is highly prone to being misused as an infringement. Developers only consider the market benefits brought by the technology and put it on the market. But when it comes to liability determination, they use the "neutral technology" as an excuse to avoid responsibility. Some scholars believe that this is not the fault of the technology itself, but rather the "original sin" of capital pursuing profits.However, the unique GAN model of deepfake technology has made the false works it generates highly realistic, enhancing the ability to infringe upon individuals. Its adversarial mode also enables it to bypass manual supervision during production. Therefore, the independence, falseness, and realistic effect of deepfake works are sufficient to draw attention to the negative effects they bring. This is also the logical point where criminal law can regulate them. We cannot ignore their impact due to the neutrality of the technology.

This one-sided perception of technological neutrality may weaken the risk prevention for the technology itself, leading to a governance tendency of "emphasizing post-event accountability while neglecting pre-event prevention". Finally, there is a lack of correct understanding of synthetic technology at the public level. The public lacks vigilance against the risks brought by emerging technologies. Most users merely view deepfake technology as an "entertainment tool" or an "emerging technology", failing to realize the possible chain reactions it may cause, such as when using a face-swapping mini-program, they accepted the conditions of the other party collecting their facial information out of momentary curiosity, increasing the low risk of their own information leakage or the public might spread AI-forged celebrity privacy videos or government documents out of curiosity, or even ignoring the main body's face in pornographic deepfake, neglecting the mental damage suffered by the victims. The majority of the public lacks a sense of crisis and fails to recognize the harm caused by the abuse of such technologies, such as potentially fueling cyber violence, damaging the reputation of the parties involved, and undermining the foundation of social governance.

3. The Legal Protection Path for Deepfake Technology

3.1 Solving the Application Problems of the Legal System

Firstly, the scope of protection for personal information should be expanded. The law should keep up with the times. We should not be confined to its surface or traditional meaning. False personal information still infringes upon the rights and interests of the information subject. If only civil and administrative measures are used to solve this problem, it is insufficient to combat this harmful behavior. Therefore, issues related to the authenticity of information and biometric identification brought about by deepfake technology should be included in the protection scope of the crime of infringing upon citizens' information. Currently, we can incorporate "biometric information generated by deepfake and capable of identifying a specific identity" into the protection objects of Article 253-1 of the Criminal Law through judicial interpretation. Just like in the criminal incidental civil public interest lawsuit case of Li Kaixiang for infringing upon citizens' personal information, the judge clearly stated that "identifiable" information belongs to the citizens' personal information as stipulated in the Criminal Law.Secondly, there are viewpoints suggesting that measures should be taken to regulate such acts of committing other crimes through the addition of relevant identity-related crimes.However, there are also different opinions on this. The affirmative side believes that this is a form of identity fraud, and its essence is actually identity theft, and in order to strengthen the protection of biometric

information, it is necessary to add relevant crimes such as identity fraud and other related crimes to regulate its independent illegality. While the opposing side believes that the deep-faking technology itself should not be directly regarded as a criminal regulation object in the criminal law.Because the illegality of the act will be absorbed by the subsequent related criminal acts, we should determine the criminal responsibility based on the specific purpose and nature of the behavior of the perpetrator using forged information, rather than treating the technical generation process as a separate crime. Therefore, the mere act of forging information itself does not necessarily have punitive nature. Some scholars also believe that treating it as a separate crime essentially involves transforming the preparatory act into an actual act. This violates the principle of legal modesty and will suppress the development of emerging industries. Adding a separate crime actually runs counter to the current light-punishment concept of criminal law. Therefore, a more appropriate legislative solution is to add specific provisions within the existing legal framework to supplement and improve it. For example, an additional clause could be added to Article 253-1 of the Criminal Law, stating that if one illegally uses deep forging technology to create others' biometric information for identity fraud, deception, and other criminal activities, they shall be punished more severely in accordance with the provisions of the previous paragraph.This not only can limit the scope of criminal liability, only punishing the acts "used for illegal activities", leaving room for development of legal purposes such as research and artistic creation, but also can avoid establishing a separate new crime, preventing redundant charges, and at the same time can clearly define the particularity of "biometric information", strengthening the protection of citizens' core personal rights and interests.

3.2 Improve the Regulatory Responsibility System

Firstly, enhance the implementation of laws. While strengthening the regulatory capabilities of public authorities, it is also necessary to promote cross-departmental joint law enforcement. The Cyberspace Administration of China, the Ministry of Public Security, and the State Administration for Market Regulation should collaborate to establish a biometric data regulatory platform to monitor the compliance of enterprises' data in real time. For enterprises that illegally collect or abuse biometric data, they should be subject to heavy fines and restrictions on industry entry, thereby protecting the safe use of data. Secondly, optimize the platform review and responsibility mechanism, establish a hierarchical review mechanism and strengthen responsibility assumption. The review mechanism should establish a high-risk, medium-risk, and low-risk three-level mechanism. For content involving national politics, economy and finance, public healthcare, judicial practice, etc., which will have a significant impact on society, it will be classified as the high-risk mechanism. At this time, two layers of review are required, first by the regulatory personnel for identification, and if there are still doubts about the authenticity, then it will be sent to experts for review and judgment; the medium-risk is entertainment face-swapping and voice-swapping games, commercial advertisements, literary works, etc., which are non-malicious fake content. At this time, algorithm recognition can be used for review, and at the same time, sampling manual re-examination can be conducted to save time and protect the development of the innovative industry; the low-risk is AI product content that has been significantly marked. Here, only the user's self-declaration that the product is AI-generated is required, and algorithm tools can be used to re-check whether it involves political security, pornography, etc., and no longer need to conduct manual identification, to improve the review efficiency. In addition, attention should be paid to responsibility assumption and strengthening review obligations. For suspected infringement behaviors, timely review and notification to the publisher and the victim should be conducted, and the infringement evidence should be retained on the monitoring platform. The infringer should be subject to credit punishment and included in the blacklist. For suspected infringement content reported by the public, timely review and corresponding handling should be carried out. For example, if the known infringing content has not been removed within 48 hours, it will bear joint liability. The safe harbor principle should be reasonably applied, and it cannot be used as a reason to evade regulatory obligations. In addition to the "notification - deletion" obligation, attention should also be paid to the security order of network operation, and criminal

activities should not be allowed to proceed within the legal net. Finally, the platform should also strengthen international cooperation and public education. By drawing on the successful experiences of other countries in regulating deepfake technology products, to understand the development and application of regulatory technologies, thereby improving the regulatory level of our country.

3.3 The Beneficial Governance Path of Deep Forging

Some scholars suggest establishing a digital moral order for the synthetic society based on ethics, that is, instead of focusing solely on optimizing the technology, more emphasis should be placed on the foundation construction of social cognition. Through the value guidance and behavioral constraints of ethical norms, the entire process management of the research and implementation, application practice and dissemination mechanism of synthetic technology should be improved. At the beginning of technological research and development, it is necessary to particularly strengthen professional ethical norms. By leveraging non-mandatory governance tools such as reputation governance systems and qualification reviews, high-quality requirements of the industry should be integrated into technological research and development. At the same time, it is also possible to attempt to incorporate the consensus-based ethical principles reached by humans into the algorithms, and let them self-upgrade to achieve the evolution from abstract ethics to practical operability. For developers, it is necessary to clearly define their reasonable foresight obligation. Ethical review should be directly incorporated into the technological research and application process, requiring enterprises to conduct ethical risk assessment before launching deep forging-related products, and reasonably foresee potential problems and configure appropriate solutions, while publicly disclosing the assessment results. Regarding the impact of deep forging on personal privacy, a specialized database early warning mechanism can be established. By combining with the police, internet enterprises' data, a high-risk population database can be constructed. For abnormal deep synthesis behaviors, automatic early warnings can be issued. Referencing the high-risk content priority review principle of the EU's "Digital Services Act", platforms are required to implement a 24-hour response mechanism for deep forging content involving women. At the same time, the evidence rules for protection can be optimized. The rule of reversing the burden of proof can be attempted to be applied. Letting the dissemination platform prove that it has fulfilled the reasonable review obligation can avoid the victim bearing high technical proof costs. At the public level, the digital literacy and artificial intelligence ethics literacy of all citizens should be enhanced. Through public media, school education, community platforms, etc., the principles and risk cases of deep forging technology and its risks should be popularized, enhancing public awareness of prevention. By creating public-friendly AI fraud public welfare short videos, using real cases to demonstrate how to identify voice cloning, video face-swapping, and other common forgery methods, and actively establishing a public governance mechanism, encouraging public reporting of deep forging infringement behaviors, and rewarding valid clues can foster a social atmosphere of formation.

References

[1]Madhura Thombrei, Deconstructing Deepfake: Tracking Legal Implications and Challenges, International Journal of Law Management & Humanities,2021, Vol. 4 Iss. 4, p. 2267.

[2]Robert Chesney, Danielle Keats Citron, 21st Century - Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security, Maryland Law Review, Vol.78,No. 4, p.884, Pp.884-885.

[3]Wang Lusheng. On the Integrated Regulation of "Deep Fakes" Intelligent Technology [J]. East Asian Legal Studies, 2019, (06): 58.

[4]Li Teng. Construction of the Criminal Regulation System for "Deep Fakes" Technology [J]. Zhongzhou Academic Journal, 2020, (10): 54.

[5]Please refer to the second-instance criminal ruling document No. 333 of the Intermediate People's Court of Quzhou City, Zhejiang Province (2019).

[6]Please refer to the Criminal Judgment No. 36 of 2023 of the Huangdao District People's Court of Qingdao City, Shandong Province.

[7]Zheng Gaojian. Criminal Responses to the Abuse of Deepfake Technology [J]. Legal Science (Journal of Northwest University of

Political Science and Law), 2025, 43 (03): 68.
[8]Yue Haishong. Understanding and Application of the Judicial Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on the Crime of Infringing upon Citizens' Personal Information [M]. Beijing: China Legal Press, 2018: 4-5.
[9]Li Huaisheng. Criminal Sanctions for the Abuse of Personal Biometric Information: A Case Study of "Deep Fakes" in Artificial Intelligence [J]. Political and Legal Forum, 2020, 38 (04): 154.
[10]Wen Ming, Sun Yuanyuan. Research on Risks and Legal Regulation of Deep Fakes Technology Application [J]. China Science and Technology Forum, 2023, (04): 162.
[11]Lin Aijun, Lin Qianmin. The Technical Risks and Diversified Regulations of AI Face Swapping [J]. Future Communication, 2023, 30 (01): 60-69.
[12]Chen Ran. Criminal Regulation of Deepfake Information Involving Sexual Content [J]. Law, 2024, (03): 86.
[13]Supreme People's Court Guiding Case No. 192: Criminal and Civil Public Interest Litigation for Infringement of Citizens' Personal Information by Li Kaixiang
[14]Li Teng. "The Construction of Criminal Regulation System for 'Deep Faking' Technology" [J]. Zhongzhou Academic Journal, 2020, (10): 57.
[15]Li Huaisheng. Criminal Sanctions Thoughts on Abusing Personal Biometric Information - Taking Artificial Intelligence "Deep Faking" as an Example [J]. Political Science and Law Forum, 2020, 38 (04): 151.
[16]Jin Lijia. As a Type of Illegal Participation in Crimes - Also Discussing the Illegality of the Act of Illegally Publishing Deep Faking Information [J]. Journal of East China University of Political Science and Law, 2020, 23 (06): 77.
[17]Li Minglu. "The Criminal Governance Path of Deep Forging [J]. Science and Law (Chinese and English), 2021, (06): 40.
[18]Liu Xianquan. Criminal Regulation of Deepfake Behaviors in the Era of Artificial Intelligence [J]. Politics and Law, 2025, (11): 60.
[19]Liang Yilan. Research on Legal Protection of Citizens' Personal Information Based on Facial Recognition Technology [J]. Western Journal, 2024, (12): 92-95.
[20]Zhang Xin, Song Yuxin. The Gender Ethics Dilemma and Governance Path of Deep Forging: A Study on Algorithmic Gaze [J]. Women Studies Review, 2024, (06): 87.
[21]Li Xueyao. The Legal Nature of Artificial Intelligence Ethics [J]. Chinese and Foreign Law Journal, 2024, 36 (04): 884-898.