The Dilemma and Path Optimization of Criminal Law Regulation for Generative Artificial Intelligence Deep Forgery

Jinghan Shi *

School of Politics and Public Administration, China University of Political Science and Law, Beijing, 102249, China

* Corresponding Author Email: 250404063@cupl.edu.cn

Abstract. The rapid development and inclusion of generative Artificial Intelligence (AI) technology have greatly reduced the threshold of deep forgery production. Its abuse has posed multidimensional and deep-seated harm to civil rights, social order and even national security. The intervention of criminal law has become inevitable and urgent. In judicial practice, the application of charges is diversified and inconsistent. Due to the lack of distinction between the essence of deep forgery, the application of law is fragmented, which leads to differences in the standards of conviction and sentencing, and different judgments in the same case. At the same time, the existing provisions of criminal law have significant limitations, which are reflected in the obvious application obstacles and legislative lag when dealing with the problem of deep forgery of generative AI. In view of the above problems, the article proposes to optimize the path of criminal law regulation from the two aspects of legislation and justice, expand the interpretation of charges in legislation, unify the judgment standards in justice, and improve the regulation efficiency. Through the above means, people can enhance the credibility and effectiveness of criminal law regulation and build a deep counterfeiting criminal law response system in the era of generative AI.

Keywords: Generative AI, deep forgery, criminal law regulation, application of charges, referee criteria.

1. Introduction

In recent years, generative Artificial Intelligence (AI) technology represented by generative counterwork networks and diffusion models has made a revolutionary breakthrough. It has migrated from the initial simple image style to the ability to generate fake videos and highly realistic voice clones that confuse the real with the fake. Generative AI has improved the efficiency of generating content. Although the application of deep forgery in comedy, advertising, marketing and other scenes can be regarded as positive and harmless, the reality is that its use in other scenes may pose a very dangerous threat: it can tamper with facts, but also because of the availability and abuse of its technology, it will erode public trust and trigger a global crisis [1,2].

In order to solve the global challenges brought by the deep forgery technology, internationally, laws such as the artificial intelligence act have been promulgated one after another, and its focus is shifting from pure technology governance to the protection of personality rights in the virtual world. In contrast, although the existing research in China has recognized the social harm caused by deep forgery, the content related to generative AI in the existing data security law and other laws has not been improved. China's legal norms adopt the terms of "deep synthesis" and "generative artificial intelligence". This "technical" expression, to a certain extent, weakens the evaluation of the social harmfulness of "deep forgery" as a criminal phenomenon, and weakens the negative effects of deep forgery with the neutrality of technology. This position has also had an impact on the research vision of legal researchers. Most of the existing discussions in the criminal law circle are based on the macro analysis of the possibility of criminalization of technology abuse [3]. In the face of this situation, it is necessary to further clarify where the lack of adaptability between the charges of forgery, infringement of citizens' personal information, network crime and deep forgery in the current criminal law is reflected, how to balance the boundary between technological innovation and criminal regulation, and build a criminal regulation path of deep forgery that fits China's legal system and has both pertinence and operability.

2. The Current Situation and Dilemma of the Application of Deep Forgery in China's Criminal Law

2.1. Analysis of the Application of Charges

The current judicial practice shows obvious characteristics of diversification and disunity in the application of charges. In the case of AI face changing video production, the judicial organ will apply article 253-1 of the criminal law to the crime of infringing on citizens' personal information. For example, in the case of Qin Xiaolong, Zhou Shiji and Han Shuai's infringement of citizens' personal information, the defendant used AI face changing, light and shadow magic hand, CT8 and other software and technologies to authenticate the Baijia number of citizens' personal information and sold the Baijia number for profit through the network platform. The court held that the acts of the three people constituted the crime of infringing citizens' personal information [4]. In the cases involving the production of pornographic videos of AI face changing, the judicial organs tend to apply the crime of making, copying, publishing, selling and disseminating pornographic materials for profit or the crime of disseminating pornographic materials in articles 363 and 364 of the criminal law. Fraud case of Zhou and others – be vigilant against using AI face changing and voice changing technology to cheat the elderly. The court held that the defendant Zhou and others fabricated facts, concealed the truth, and defrauded others' property for the purpose of illegal possession. The amount was large, and their behavior constituted the crime of fraud according to Article 266 of the criminal law [5].

This decentralized application of charges reflects that when facing new technology crimes, the judiciary is more inclined to find the closest provisions to regulate within the current legal framework, rather than distinguish based on the nature of deep forgery in different cases. This leads to the fact that it is clearly an act of abuse of deep forgery technology, but it is classified into different charges due to minor differences in the cases, resulting in fragmentation in the application of the law.

2.2. Differences in Conviction and Sentencing Standards

The non-uniform application of charges has caused differences in sentencing standards, and the phenomenon of „different judgments in the same case" has occurred from time to time. Taking the case of AI face changing pornographic video as an example, some courts focused on protecting society and managing social order, and were convicted of the crime of disseminating pornographic materials. While the other part of the Court emphasized the infringement of the victim's personal reputation right, and tended to be punished as the crime of insult. There are significant differences between the two crimes in the threshold of incrimination and the allocation of legal penalty, which directly leads to the different penalty results of the perpetrators. Some judges insist on the traditional quantitative standards such as hits and dissemination range, and believe that deep forgery is only the upgrading of technical means, and does not change the evaluation method of harmful results; Another view is that the "authenticity" brought by the deep forgery technology makes the spiritual damage of the victim far more serious than the traditional libel cases. This separation of judicial logic exposes the lack of awareness of the technical characteristics of deep forgery in the judicial system, as well as the adaptability dilemma of the traditional sentencing standards in the face of new forms of harm.

2.3. Limitations of Existing Criminal Law Provisions

Current criminal law has obvious application obstacles and legislation lags in dealing with generative AI deep forgery. Crimes such as insult and libel are mainly private prosecution, while deep forgery involves technical black box, which makes it difficult for victims to provide evidence and obstructs the channel of safeguarding rights. The regulation of "production" and "communication" in criminal law is separated, and the behavior of pure production without communication is basically in the blank of regulation. The harm of deep forgery spreads quickly, the damage is invisible, the scope of transmission and impact are difficult to quantify, and the existing conviction standards cannot be accurately measured. At the same time, the defense of "technology neutrality" in the judiciary is often

abused, and the criminal law lacks special rules of accountability for technology providers, resulting in insufficient basis for liability determination. Therefore, in the face of the technology driven crime of deep forgery, the traditional charge system has shown obvious lag and insufficient adaptation. It is urgent to build a more targeted and forward-looking criminal law response system through the improvement of legislation or judicial interpretation.

3. Suggestions on Path Optimization of Criminal Law Regulation

3.1. Improving the Regulatory System and Filling the Legal Gap

The principle of a legally prescribed punishment for a specified crime is the basic principle of China's criminal law. Its core meaning is "no crime without explicit provisions of the law, no punishment without explicit provisions of the law". This principle is not only the cornerstone to protect citizens' personal and property rights, but also the core criterion to limit the abuse of judicial power and maintain legal stability.

There are many controversies on whether special legislation should be made for deep forgery cases in the international community. Most countries have no special charges and rely on traditional criminal law. For example, Germany, Poland and other countries have not made special legislation for deep forgery but have made special regulations for a certain law article. However, a few countries have made special legislation or explicitly criminalized it. For example, Denmark, Sweden and other countries have clearly criminalized the production and dissemination of undesirable deep forgery [6,7].

For China, in order to maintain the stability of the Chinese legal system, it is still necessary to make targeted and expanded interpretation of the charges in the criminal law to fill the gap in the application of existing charges for the different types of behavior and the infringement results of legal interests of the abuse of deep forgery technology. For example, in view of reputation infringement, the legislation should make it clear that those who simply make fake audio and video with the intention of insulting or slandering others will be held accountable in preparation for a crime. Even if the spread content does not reach the scale of traditional slander, as long as it causes serious mental damage, it can be used as the core basis for criminalization and heavier punishment [8]. In view of the abuse of biological information, the use of biological features such as unauthorized capture, training, synthesis of other people's faces and voice prints for deep forgery should be fully included in the criminal regulation. For the technical assistance behavior, it should be clear that the algorithm, tool and platform providers who knowingly provide support for others' illegal deep forgery will be punished as accomplices. Those who provide upstream and downstream services such as model training, data processing, distribution and drainage for the deep forged black industry chain will be investigated for criminal responsibility [9]. In view of the harm to public order, the fake audio and video of government affairs, disaster and people's livelihood should be included in the category of "false information". If such content is produced and disseminated with the intention of disturbing public order, criminal responsibility will be directly investigated.

3.2. Unifying the Judgment Standards and Improving the Regulation Efficiency

The improvement of legislation needs effective practice of justice. People can promote the standardization construction at the judicial level from the aspects of evidence rules and judgment standards, so as to achieve the same case and judgment, and improve the consistency and credibility of judicial judgment.

The core difficulty of deep forgery cases of generative AI lies in the identification of electronic evidence. Because the content of deep forgery is highly realistic, traditional identification methods are difficult to effectively identify, and electronic evidence is easy to be tampered with and difficult to trace, resulting in difficulties in identifying the authenticity and legitimacy of evidence. Combined with the current situation of judicial practice, people should first clarify the identification standard of deep forgery of electronic evidence. The Supreme People's court will issue relevant judicial

interpretations to clarify the key points of the review of in-depth forged electronic evidence, including the source of evidence generation, transmission path, tampering traces, expert opinions, etc. However, attention should be paid to avoiding the influence of "technology omnipotence" and "total skepticism", that is, it is enough to have AI detector and audio-visual evidence in the era of deep forgery should not be adopted in principle. In fact, the accuracy of the detector is limited, and the attack and defense will continue to upgrade. It cannot rely on technology to solve judicial problems. The "total skepticism" will also lead to the exclusion of a large number of true key evidence, seriously damaging the function of judicial discovery of truth [10]. At the same time, it is also necessary to optimize the allocation rules of the burden of proof, which is also a key measure to deal with the problem of AI falsifying evidence.

The disunity of judgment standards is one of the most prominent problems in the current judicial practice of deep forgery cases. The same type of cases may have different judgment results in different regions and different courts, which seriously affects the judicial credibility. Therefore, it is necessary to unify the judgment standards in a variety of ways. The Supreme People's court should unify the judgment standards of deep forgery cases through judicial interpretation and guiding cases. For example, because personal sexual life and political activity information are sensitive data, deep forgery content containing such information will be prohibited unless the parties explicitly agree, and consent is usually unavailable in deep forgery scenarios. For the deep forgery of non-sensitive information, people should adhere to the principle of consent of the parties and legalize the exception as an exception. Only when the public interest is involved and the right of personality is not infringed, can there be restrictions on its application. At the same time, typical cases of in-depth forgery are selected as guidance cases and released to courts across the country to provide reference for courts at all levels to try similar cases and solve controversial issues in judicial decisions, such as clarifying the distinction between the crime of insulting and the crime of obscene articles, determining the nature of "face information" in the crime of infringing on the personal information of citizens, and paying more attention to mental damage, scope of transmission and deception in sentencing. The court should also strengthen the professional training of judicial personnel. The generative AI deep forgery technology has strong professionalism. The lack of awareness of technology by judicial personnel is an important reason for the disunity of judgment standards. Therefore, judicial personnel should be regularly organized to carry out professional training, including the principle of generative AI technology, the identification method of deep forgery, and the identification technology of electronic evidence, so as to improve the technical literacy and case trial ability of judicial personnel.

For difficult and complex cases of in-depth forgery, a coordination mechanism should be established between higher and lower courts and between courts at the same level to strengthen communication and exchange and unify the trial ideas and judgment standards. In the case of dispute, the superior court can provide guidance to avoid judgment conflict. At the same time, people should strengthen the legal supervision of procuratorial organs, protest against cases with inconsistent judgment standards and wrong application of law according to law, ensure the fairness and consistency of judicial decisions, enhance judicial credibility, respond to the public's expectation of a fair trial of deep forgery cases, and safeguard social fairness, justice and legal authority.

4. Conclusion

As a typical example of the abuse of generative AI technology, the social harm of deep forgery cannot be ignored. When dealing with this new type of crime, the current criminal law is facing multiple difficulties, such as the fragmentation of charge application and the divergence of sentencing standards, which exposes the lack of adaptability of the traditional criminal law system in dealing with technical crimes. The root cause lies in the fact that the criminal code does not grasp the essential characteristics of deep forgery and fails to fully respond to the infringement of legal interests brought by its "authenticity", "easy diffusion" and "technical concealment".

In order to solve this dilemma, people should promote it from legislative and judicial levels. Legislation, through the expansion of the crime of insult, the crime of infringing on citizens' personal information, the crime of illegal use of information network and other charges, to fill the regulatory gap. Judicially, people should unify the standards for the identification of electronic evidence and the rules for conviction and sentencing, give play to the exemplary function of guiding cases, and strengthen the technical training of judicial personnel. Only by clarifying the dual path of "legislation + justice", can people effectively curb the deep forgery and abuse, and safeguard the rights and interests of citizens, social order and national security while ensuring the space for technological innovation.

References

[1] Hasan H. R., Salah K., et al. Combating Deepfake Videos Using Blockchain and Smart Contracts. IEEE Access, 2019, 7: 41596-41606.

[2] Lanham M. Generating a New Reality. Springer, 2021.

[3] Chen R. Criminal law regulation of deep forgery of sexual information. Law, 2024, (03): 76-90.

[4] Ganyu District People's Court Lianyungang City Jiangsu Province. Su 0707 xingchu No. 180: Qin Xiaolong, Zhou Shiji, hanshuishuai criminal judgment of first instance on the crime of infringing on citizens' personal information. 2021-04-29.

[5] National Internet Information Office, Ministry of Public Security, Ministry of Civil Affairs. The fourth typical case of the protection of the rights and interests of the elderly in China in 2024: beware of using AI face changing and voice changing technology to cheat the elderly. 2025-04-29. http://www.cac.gov.cn/2025-04/29/c_168861694.

[6] Bień-Węgłowska I., Tuora-Schwierskott E., et al. Deepfake and Selected Crimes in Polish and German Criminal Law. Teka Komisji Prawniczej PAN Oddział w Lublinie, 2025, 18(2): 35-49.

[7] Yavuz C. Criminalisation of the dissemination of non-consensual sexual deepfakes in the European Union: A comparative legal analysis. Revue Internationale de Droit Pénal, 2024, 95(2): 419-457.

[8] McGlynn C., Toparlak R. T., et al. The 'new voyeurism': criminalizing the creation of 'deepfake porn'. Journal of Law and Society, 2025, 52(2): 204-228.

[9] Yavuz C. Criminalisation of the dissemination of non-consensual sexual deepfakes in the European Union: A comparative legal analysis. Revue Internationale de Droit Pénal, 2024, 95(2): 419-457.

[10] Cheng E. K. Deepfakes, Photographs, and Trust in Evidence. Virginia Law Review Online, 2025.