Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD29522

The Dilemma and Way Out of Criminal Regulation on Deepfake Sexual Information

Qiyun Li

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan, China
202421050046@stu.zuel.edu.cn

Abstract. With the rise of deepfake technology, criminals are exploiting AI face-swapping to disseminate sexual information, severely infringing on citizens' sexual privacy and personal dignity. However, existing laws often charge such actions under the crime of disseminating obscene materials, leading to issues such as misapplication of charges and vague determination of responsibility. This study identifies three main difficulties in current criminal law regulation: First, the misapplication of existing charges, which either ignore the main intent of the crime or fail to fully consider the adverse effects of the dissemination of obscene videos. Second, the imprecise positioning of legal interests protection, which focuses on macro legal interests rather than core individual legal interests such as sexual privacy and personal dignity. Third, the vague standards for determining criminal responsibility, with unclear boundaries among various participating entities. To address these issues, this study proposes three solutions: First, improve legislation by adding the crime of "deepfake sexual information" to clarify the scope of regulation and achieve precise protection of citizens' rights. Second, refine judicial determination standards by holding criminals accountable based on subjective intent, the role of the behavior, and the harmful consequences. Third, strengthen legal coordination and governance through administrative law to regulate technology, civil law to provide remedies, and criminal law to intervene when necessary, forming a comprehensive governance system to address the social harm of deepfake sexual information.

Keywords: Deepfake, Sexual Information, Criminal Regulation

1. Introduction

Deepfake is a portmanteau of "deep learning" and "fake," referring to the simulation and forgery of audio and video using deep learning algorithms. The core of deepfake technology is the Generative Adversarial Network (GAN), which, through the adversarial iteration of a generator and a discriminator, can synthesize highly realistic non-authentic audio and video. This technological characteristic makes deepfake sexual information more likely to deceive and thereby exacerbates the infringement of victims' rights [1]. In June 2023, Bai from Beijing came into contact with the "one-click clothing removal" technology on an overseas social media platform and intended to profit from it. He used AI software to deeply forge victims' images, generating obscene images in batches within seconds or minutes. Bai sold these images to 351 people on QQ, with nearly 7,000 images sold at a

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.LD29522

price of 1.5 yuan per photo. Such behavior not only severely affects social morality but essentially infringes on citizens' sexual privacy and personal dignity. From June 2021 to June 17, 2022, the defendant Zhang Long, with the purpose of making a profit, uploaded multiple AI face-swapped obscene videos he had made to an overseas website and posted his QQ number on the obscene videos to seek clients. However, the defendant Zhang Long was charged with the crime of producing, selling, and disseminating obscene materials for profit, ignoring the protection and emphasis on the personal rights of the victims during the crime. This also indirectly indicates that the existing legal system often simply charges such actions under the crime of disseminating obscene materials, lacking protection for citizens' sexual privacy and personal dignity.

From a global regulatory perspective, deepfake sexual information has attracted legislative attention in many countries. In 2018, the U.S. Senate proposed the "Malicious Deepfake Prohibition Act," and in 2019, the House of Representatives proposed the "Deepfake Accountability Act"; the EU included "deep synthesis" in the "General Data Protection Regulation (GDPR)," adopting a data governance and algorithm regulation model, and also issued the "EU Code of Practice on Disinformation." Germany, Singapore, the UK, South Korea, and other countries have attempted to incorporate deepfake into the criminal law category. Although China's "Provisions on the Administration of Deep Synthesis of Internet Information Services" and "Interim Measures for the Administration of Generative Artificial Intelligence Services," implemented in 2023, are legislatively advanced in the governance of deepfake, there is still room for improvement in criminal regulation [2].

Therefore, analyzing the dilemmas and solutions in the criminal regulation of deepfake sexual information crimes has become an urgent task. This article mainly starts from the defects in the existing criminal law's regulation of deepfake sexual information, analyzes the specific manifestations of the existing criminal regulation defects from three aspects: the misapplication of existing charges, the imprecise positioning of legal interests protection, and the vague standards for determining criminal liability. It then proposes targeted governance measures from three aspects: improving legislation, refining judicial determination standards, and strengthening the coordinated governance effects of different laws, to effectively regulate such criminal behavior and make up for the defects and loopholes in the existing criminal law.

2. The dilemma of criminal regulation on deepfake sexual information

2.1. Misapplication of existing charges

In current judicial practice, the behavior of deepfake sexual information is mostly characterized under traditional charges such as "disseminating obscene materials." However, the core legal interests infringed by deepfake sexual information are citizens' sexual autonomy, privacy, and personal dignity, and the illegal essence of the behavior is rooted in the non-voluntary misuse of images through "deepfake." In contrast, traditional charges like disseminating obscene materials tend to focus on behaviors that disseminate content with sexual information, resulting in certain deviations in the application of charges. For example, in real life, many people, out of a desire for revenge, use AI face-swapping and audio processing to replace the main characters in obscene videos with the appearance and voice of the victims and then disseminate the videos through social platforms. In this process, the main purpose of the criminals is not to disseminate obscene videos but to use them to illegally infringe on the victims' rights to reputation and personal dignity. Jessica Reilly also pointed out that the core harm of deepfake sexual information is not the "destruction of social morality by the dissemination of obscene content" but the deprivation of citizens' control over

DOI: 10.54254/2753-7048/2025.LD29522

their sexual identity through technical forgery means. This type of infringement has three characteristics: "virtuality, targeting, and irreversibility," which are fundamentally different from the logic of legal interest infringement in traditional obscene material crimes that only disrupt abstract social order [3].

Moreover, deepfake sexual information behavior is also difficult to be fully evaluated by other existing charges. Although deepfake sexual information targets the "identifiability" of specific natural persons, it does not fall under the false emergency, epidemic, disaster, or police information in the charge of fabricating and deliberately disseminating false information, and thus cannot be applied to that charge. The crime of infringing on citizens' personal information only regulates illegal acquisition, sale, and provision. If the original data used for deepfake comes from legally public resources, it does not meet the "illegal acquisition" element of that charge [4]. Therefore, there are deviations in the application of existing charges to this type of criminal activity involving deepfake sexual information.

2.2. Imprecise positioning of legal interests protection

From the perspective of legal interests protection, deepfake sexual information mainly infringes on individual rights such as citizens' right to reputation and personal dignity. However, traditional charges like "disseminating obscene materials" often focus on protecting more macro rights such as social morality and usually fail to protect individual citizens' rights in detail. The 1999 World Association for Sexual Health's "Declaration of Sexual Rights" clearly established the independent protection status of sexual privacy rights. The core infringement of deepfake sexual information on victims lies in sexual privacy. However, China currently does not have special protection for special rights such as sexual privacy, and its protection mainly relies on indirect protection through civil law and other departmental laws. In contrast, foreign jurisdictions have more robust protections: the French Penal Code distinguishes between "infringement of private life" and "infringement of others' image"; the German Penal Code stipulates "infringement of personal life and secret domains"; and the Spanish Penal Code provides for heavier penalties for violations of sexual privacy. In many countries, the criminal law's protection of privacy is stronger than that of general reputation rights, and some even set stricter criminal penalties for sexual privacy violations [2]. In China's judicial practice, similar criminal activities are mostly charged with disseminating obscene materials, and deepfake behavior is considered an auxiliary means of dissemination, downplaying the adverse effects and negative impacts of deepfake behavior. This misalignment of legal interests protection not only fails to highlight the protection and emphasis on the core legal interests infringed by deepfake sexual information, such as sexual privacy, but also, due to the misalignment of legal interests protection, the abuse of deepfake technology in the dissemination of obscene materials lacks necessary targeting and sanctions. This misalignment objectively reduces the sanction intensity against the abuse of deepfake technology and indirectly condones the spread of such behavior in criminal activities.

In addition, the legal interests infringed by deepfake sexual information have a compound nature. In addition to the individual rights of citizens such as sexual privacy and personal dignity, it may also undermine the trust foundation of cyberspace [5]. Originally, many citizens would post pictures and videos containing personal information on online platforms based on a certain level of trust in cyberspace, such as personal life photos. However, now criminals use the information posted by others to commit illegal acts such as deepfake sexual information, using the information posted by others to infringe on their legitimate rights and interests, thereby impacting citizens' trust in cyberspace and deteriorating the cyberspace environment.

DOI: 10.54254/2753-7048/2025.LD29522

2.3. Vague standards for determining criminal liability

Regarding the allocation of responsibilities among various parties involved in the process of deepfake sexual information and the criminal liability that criminals should bear, the current standards for determining criminal liability are still vague. First, in the criminal process of deepfake sexual information, there are often multiple parties involved, such as the criminals, AI technology providers, and online platforms. However, under the existing criminal law framework, it is difficult to reasonably define the boundaries of criminal liability among these parties. The specific criminal methods of the criminals, the knowledge of the AI technology providers and online platforms, and other factors are all important and difficult to determine in such cases. Some scholars believe that there is a controversy over whether the provision of specialized deepfake technical services constitutes a joint crime with subsequent use behaviors: according to the theory of complicity, if the subsequent use behavior does not constitute a crime, the technical service provision behavior is also difficult to charge; but if it is not recognized as a joint crime, whether the "industrialized" technical service behavior can be regulated by the crime of illegal use of information networks or aiding information network crimes is currently lacking a clear standard [6].

Secondly, due to the existing problems of misapplication of charges and imprecise positioning of legal interests protection, criminals are charged with disseminating obscene materials, ignoring the illegal infringement on the victims' rights to reputation and personal dignity, and there are certain defects in the determination of criminal liability. This misalignment of criminal liability is a manifestation of the current problems in criminal regulation, and it is a chain reaction to the emergence of existing problems such as the misapplication of charges. Therefore, if the study want to reasonably regulate such criminal behavior, it should start solving the existing problems such as the misapplication of charges one by one to prevent the problem from getting worse.

3. The way out for criminal regulation on deepfake sexual information

3.1. Improve legislation and clarify charges and legal interests protection

Since existing charges fail to fully cover the illegal essence of deepfake sexual information behavior, it is necessary to add a specific charge, such as "deepfake sexual information crime." The behavior of using deepfake technology to produce and disseminate sexual information, which seriously infringes on citizens' sexual privacy and personal dignity, should be included in the scope of regulation of this charge. This can change the previous situation in which the protection of citizens' sexual privacy and personal dignity is confused with the protection of social order in such cases at the legislative level, effectively safeguarding citizens' legitimate rights and interests. It can also achieve precise crackdowns on such crimes and ensure proportionality between crime and punishment.

Of course, when adding this charge, it is necessary to clarify its elements of the crime: in terms of behavior, it should cover all aspects of using deepfake technology to produce and disseminate sexual information, including obtaining biometric information, generating false content, and disseminating through the Internet or other channels; in terms of subjective intent, the perpetrator must have the intent and must know that the behavior will infringe on others' sexual privacy or personal dignity; in terms of harmful consequences, it must reach the level of "serious circumstances," which can be comprehensively determined based on factors such as the scope of information dissemination, the degree of damage to the victims, and the number of times the behavior occurs [7]. In addition, considering that deepfake sexual information often involves the abuse of personal biometric

DOI: 10.54254/2753-7048/2025.LD29522

information, it is possible to explicitly include the illegal use of personal biometric information as one of the elements of the crime. At the same time, drawing on foreign legislative experience, a stricter criminal penalty ladder can be set for the infringement of sexual privacy to strengthen the protection of citizens' core individual legal interests [8].

3.2. Refine standards for judicial determination

When determining criminal liability, the actual actions and roles of each party in the case should be fully considered. For criminals, their criminal liability should be strictly pursued based on factors such as their subjective intent, behavior, and the harmful consequences caused; for relevant technical service providers and online platforms, reasonable and legal norms and standards should be clarified, with the review obligation being the top priority. If relevant technical service providers and online platforms fail to fulfill their reasonable review obligations, resulting in the dissemination of deepfake sexual information, they should bear corresponding criminal liability. If they have fulfilled their reasonable review obligations but criminals still manage to produce and disseminate through other means, their criminal liability in such cases should be appropriately reduced. In terms of the knowledge of the platforms, the core problem of the vague boundaries of responsibility among multiple parties in deepfake sexual information cases is that the existing criminal law does not distinguish between "technical neutrality" and "intentional abuse of technology." For platforms that specifically provide deepfake technology, if they know that users frequently upload others' portraits and generate sexual content but fail to take technical interception or account banning measures, they should be considered to have "indirect intent" and can constitute an accomplice; however, if they only provide AI tools without specific purposes and delete relevant content in a timely manner after receiving infringement notices, they should be exempt from criminal liability [9]. In addition, the judicial process can be organically combined with the legislative link, and suggestions for improvement can be provided to legislators based on actual judicial needs. Since the implementation of laws has certain lag, a trial period should be established, during which opinions from all parties should be collected, and after the end of the trial period, problems should be integrated and analyzed.

3.3. Strengthen the coordinated governance effect of different laws

Since the legal interests involved in deepfake sexual information issues and the participating parties are somewhat complex, it is not advisable to rely solely on criminal law but to fully leverage the regulatory role of different departmental laws such as civil law and administrative law to achieve coordinated cooperation among various departmental laws. The "administrative supervision - civil relief - criminal bottom-line" system formed by the EU in the governance of deepfake sexual information is worth learning from. It requires technology research and development enterprises to embed "deepfake content identification technology" (such as digital watermarking) in the product design stage. Administrative agencies regularly conduct compliance inspections to urge platforms to fulfill their review obligations and only initiate criminal prosecution when the behavior causes serious consequences (such as victims' suicide or large-scale dissemination of information). This tiered governance model not only avoids excessive intervention of criminal law but also achieves comprehensive protection of citizens' rights and interest [10]. This "preemptive prevention, mid-term supervision, and post-term strict punishment" tiered progressive model provides a clear blueprint for China to build a coordinated governance system. For China, administrative law should strengthen the supervision of deepfake technology research and application, regulate the AI industry

DOI: 10.54254/2753-7048/2025.LD29522

order, and reduce the occurrence of such criminal offenses at the source. It should also urge relevant administrative agencies and platforms to perform their duties and fulfill their obligations in accordance with the law; civil law should strengthen the protection of citizens' sexual privacy and other special rights, shifting from indirect protection to direct protection of such special rights, providing civil relief channels for victims, and reducing the adverse social impact of such behavior on victims to a certain extent. Criminal law, as a safeguard law, should intervene in a timely manner when administrative law and civil law fail to effectively regulate, severely crack down on such criminal offenses, and form a comprehensive, multi-level governance system to jointly address the social harm and adverse effects brought about by deepfake sexual information.

4. Conclusion

The criminal regulation of deepfake sexual information is a long-term and systematic project that requires us to face the contradictions between technological development and legal lag, the balance between individual rights and social order, and the allocation of responsibilities among multiple parties. The current dilemmas of misapplication of charges, imprecise positioning of legal interests protection, and vague determination of criminal liability make it difficult for criminal regulation to effectively address the harm of such behavior. By adding the crime of "deepfake sexual information," refining judicial determination standards, and strengthening the coordinated governance of different laws, a targeted regulatory system can be established to achieve precise protection of citizens' sexual privacy and personal dignity while balancing technological innovation and social order stability. In the future, it is necessary to continuously improve regulatory paths in combination with technological development and judicial practice, promote the adaptation of criminal regulation to the times, and provide solid legal protection to meet the challenges brought by deepfake technology.

References

[1] Li Minglu. (2021) The Criminal Law Governance Path of "Deepfakes" [J]. Science, Technology and Law (Chinese & English), (06): 40-47+73..
[2] Chen Ran. (2024) Criminal Law Regulation of Deepfakes Involving Sexual Content [J]. Law Science, (03): 76-90.
[3] Jessica Reilly. (2022) Deepfake Pornography: A Legal and Ethical Analysis of Non-Consensual Synthetic Media [J]. Harvard Journal of Law & Technology, 35 (2): 431-435.
[4] Li Yinghan, Hou Juntai. (2025) Criminal Law Regulation of Deepfakes Involving Minors in Sexual Content [J]. Journal of the People's Public Security University of China, (03): 93-100.
[5] Jiang Ying. (2021) The Orientation and Limits of Criminal Law Regulation of the Risks of Artificial Intelligence "Deepfake" Technology [J]. Nanjing Social Sciences, (09): 101-109.
[6] Zheng Gaojian. (2025) Criminal Law Response to the Abuse of Deepfake Technology [J]. Law Science (Journal of Northwest University of Political Science and Law), 43(03): 56-68..
[7] Li Teng. (2020) Construction of the Criminal Law Regulation System for "Deepfake" Technology [J]. Zhongzhou Academic Journal, (10): 53-62..
[8] Li Huaisheng. (2020) Criminal Sanction Approaches for the Abuse of Personal Biometric Information—Taking Artificial Intelligence "Deepfake" as an Example [J]. Forum on Political and Legal Sciences, 38(04): 144-154.
[9] Neil Richards, (2021) Jonathan King. The Challenge of Deepfake Pornography to Criminal Law: Rethinking Harm, Intent, and Liability [J]. Yale Journal of Law & Technology, 23 (1): 205-208.
[10] Hyun-Jeong Kim, Luca Tosoni. (2023) Criminal Liability for Deepfake Sexually Explicit Content: Comparing Regulatory Approaches in the EU and Asia [J]. Journal of Criminal Law & Criminology, 113 (3): 594-597.