Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.32781

Research on the Criminal Regulation of the Abuse of Deepfake Technolog

Yunru Ying

Law School, Hangzhou Normal University, Hangzhou, China
3402452128@qq.com

Abstract. While deepfake technology enhances creative efficiency and interactive experience, it is also giving rise to new types of crimes. At present, criminal regulation is difficult to deal with its systemic risks due to structural flaws, and it is urgent to construct a systematic regulatory approach that is both appropriate and operational. During the information acquisition stage, the act of deepfake information collection overcomes the boundaries of citizens' personal information flow, substantially undermining the compatibility between the context and the purpose, and may constitute the crime of infringing upon citizens' personal information. During the technical processing stage, the act of using deepfake technology to process personal information essentially infringes upon the legal interests of digital identity. This can be regulated reasonably and legally by interpreting and applying the crime of illegally using information networks, independently holding the release behavior accountable. In terms of specific application, a hierarchical view of legal interests should be adhered to, and when there is a conflict or overlap between the technical processing behavior and the downstream crime, one should be chosen for treatment. At the same time, it is necessary to establish a hierarchical management responsibility system for network service providers from a comprehensive classification perspective, form a collaborative governance pattern, and achieve a dynamic balance between preventing technology abuse and ensuring innovation vitality.

Keywords: Criminal law regulation of deepfakes, Crime of infringing upon citizens' personal information, The crime of illegally using information networks

1. Introduction

With the rapid development of deep learning technology, its application in the fabrication and editing of images, audio and video has become increasingly mature. As a phased product of the evolution of artificial intelligence technology, deepfake technology has demonstrated application value in fields such as education, entertainment, and cultural and creative industries, while also opening up a new "intelligent" domain for criminal activities [1]. Many lawbreakers carry out new types of crimes such as telecommunications fraud, reputation infringement and false information dissemination through technologies like "AI face-swapping" and "AI voice-swapping". These crimes not only seriously infringe upon citizens' legitimate rights and interests such as portrait rights, reputation rights and privacy rights, but also affect the stability of social order. In this regard,

DOI: 10.54254/2753-7048/2026.32781

technical governance solutions such as "traceability and anti-counterfeiting" or "reverse cracking" often lag behind the iteration of counterfeiting technologies [2], and the focus of governance can only shift to legal norms. At present, China has established a preliminary governance framework of administrative regulation and civil constraints, providing a basis for regulating general illegal deepfake behaviors. However, the regulatory boundaries of administrative law and civil law are limited to the level of general violations. For new types of criminal acts with more serious social harm carried out by using deepfake technology, the current criminal regulation system has exposed structural flaws.

In view of this, this paper attempts to start from the risk deconstruction of deepfakes, examine the regulatory blind spots in the current criminal law regulatory system, and by comparing different regulatory paths in theory, attempt to construct a systematic and hierarchical criminal law regulatory scheme centered on the full-chain risk evaluation, with the aim of providing theoretical support and institutional references for the systematic governance system of deepfakes technology.

2. Risk deconstruction of deepfakes

2.1. Risk patterns of deepfakes

Deepfake risks exhibit systematic characteristics interwoven with technical features, application scenarios and social environments. Based on the differences in the subject's goals and scenarios, they can be classified into three categories: low-risk and non-malicious, medium-high risk and profit-driven, and high risk and political [3]. Technical researchers mostly use traditional scenarios where the goals are legal and the harm is controllable. Market entities and malicious users are concentrated in fields such as social interaction, finance, business, and creation, with the aim of making illegal profits, which may trigger a chain of harms at the market, economic, and social levels. Political subjects focus on political participation and news media scenarios, possess the ability to forge on a large scale, and directly threaten national political security and ideological stability. However, explicit classification only presents the surface, while the deep structure reveals the complex composition of risks. By applying a hybrid research method combining case studies and grounded theory, the characteristics of the interweaving of nested endogenous risks and hierarchical derivative risks in the technical hierarchical architecture of risk pattern presentation are revealed [4]. At its root, endogenous risks stem from the inherent characteristics and evolution logic of the technology itself, while the application, abuse or misuse of technology triggers derivative risks. The generation, amplification and diffusion of deepfake risks are complex dynamic processes caused by the joint action of multiple factors such as technology, system and environment.

2.2. Technical logic for the generation of deepfake risks

The risk of deepfake stems from the imbalance between technical characteristics, development behaviors and the social relationship of technology. It is based on generative adversarial networks and uses deep learning models to intelligently reconstruct multimedia content, achieving a "deceptive" forgery effect. At present, the academic community has not yet formed a unified definition of deepfake technology. Some scholars distinguish between creational deepfake technology and tamper-based deepfake technology based on whether a prototype exists or not [5]. It should be made clear that deepfake technology has certain differences from text-to-video technology [6]. Unlike the diffusion model-driven text-to-video tools that generate brand-new dynamic scenes from scratch, deepfake technology focuses on the tampering and replacement of existing content,

DOI: 10.54254/2753-7048/2026.32781

and is more targeted and dependent. At the technical implementation level, deepfake relies on generative artificial intelligence models, and its core support is massive data [7], while the first-generation datasets were usually personal sensitive information without valid consent or anonymization processing. Take AI face-swapping as an example. The original input is facial data from online videos or existing images. Neural network algorithms recognize, extract and compare and verify biological features such as the distribution of facial features, expression details and skin textures, and ultimately achieve precise grafting of facial features. From the perspective of technological evolution, its development has gone through continuous iterations from the shared weight autoencoder to the Generative adversarial network (GAN), and then to various GAN improvement models. The forgery effect has become increasingly realistic and difficult for the human eye to distinguish [8]. The leap in technological capabilities has directly driven a leap in risk management capabilities, and its popularization has also brought about impacts and challenges to social order.

2.3. Institutional predicament of risk amplification in deepfakes

First, the formalization of front-end supervision. The general public has an inherent social vulnerability in self-protection of personal information. The technical characteristics of the collection of citizens' personal information are in essential conflict with the logical premise of the "right to consent" regulatory model, which leads to the virtualization of the right to consent and poses a systemic risk to the protection of users' rights and interests [9]. If the collection of facial information in public scenes is concealed, it is difficult for users to know and refuse. The tacit approval is only for program verification rather than substantive consent. The dual risks of knowledge barriers and formalization of consent lead to the substantive virtualization of the right to consent. There are even cases where long-term and extensive usage rights are obtained through "initial consent", and the person being collected loses subsequent control. Subsequent abusive behaviors are difficult to supervise due to the fact that "consent has been reached", which leads to the intangible expansion of the rights of the collectors and the substantive damage to the rights of the collected, resulting in an imbalance of rights and interests. This regulatory failure has led to risks being breached at the entrance, opening the door to the abuse of technology.

Second, the fragmentation of judicial decisions. The current judicial practice's response to deepfake behavior shows a distinct fragmented feature. Through a review of typical judicial cases in recent years, two prominent issues can be identified. The first is the significant phenomenon of different judgments for the same case, where similar behaviors are classified as different charges in different courts. Second, there is a lack of a full-chain evaluation perspective. Referees either focus on upstream information infringement or on specific downstream crimes, and there is rarely an integrated evaluation of the harm throughout the entire process. This fragmented evaluation is difficult to cover the re-legitimate rights and interests infringed upon by deepfake behavior on personal digital identities, social trust order and even cyberspace security, leading to disorder in the transmission of risks, which may result in a mismatch between crime, responsibility and punishment, and make it hard for the deterrent function of the law to be effectively exerted.

Third, the limitations of post-event relief. The consequences of the infringement of legal interests by deepfakes have a certain degree of irreversibility, and post-event relief is not the optimal strategy. Theoretically, the general preventive function of criminal penalties can meet this demand for pre-governance, effectively curb potential illegal and criminal activities, and thereby reduce the abuse of deepfake technology at the source [10]. However, traditional criminal law theory faces significant limitations of The Times after entering the information society. The weakening, alienation and

DOI: 10.54254/2753-7048/2026.32781

virtualization effects of cyberspace on traditional criminal law from conceptual categories to basic theoretical frameworks, coupled with the extremely rapid iteration speed of cyber crime forms, have led to the predicament of systematic lag and insufficient rule supply in the criminal law system.

3. Theoretical review of the abuse of criminal law regulation by deepfake technology

3.1. Criminal law characterization of deepfake information collection behavior

Algorithm governance mainly falls within the scope of technological development, while the focus of criminal law regulation should be on data governance and application scenario restrictions. As a result, there is a controversy in the academic circle over how to protect personal information that is legally obtained but used for illegal purposes. Some scholars advocate that, given the huge social risks posed by the abuse of deepfake technology, the front-end protection of personal biometric information should be strengthened. Opponents, however, argue that deepfake audio-visual data cannot be directly criminalized due to insufficient identifiers, and that legally obtaining public information for model training itself does not constitute illegal acquisition.

However, the traditional protection framework centered on "informed consent" has become difficult to cope with the diverse scenarios of the big data era, and there is an urgent need to shift from static compliance to dynamic risk control [11]. Based on the theory of contextual integrity, the protection of sensitive personal information in criminal law should be judged based on the initial scenario defined by "metadata". This not only requires an ontological analysis of the metadata itself, but also needs to assess its normative significance in accordance with the evolving social and technological environment [12]. Any change to the core elements such as the information subject and the purpose of use, if its scene relevance and the resulting real risks have reached the threshold of criminal regulation, may constitute an infringement upon the sensitivity of the information. At this point, while recognizing the dynamic utilization value of the data, the specific criminal criteria should be established by clarifying the boundaries of improper changes.

The situational integrity theory assesses aggressiveness through four steps: First, it judges privacy based on the specific relationships among information participants; Second, determine the situational boundaries based on common interests; Third, clarify the scope of retention of privacy interests in sharing; Fourth, incorporate variables such as interest relations and ethical values into the assessment of new scenarios [13]. In deepfake scenarios, regardless of whether the initial acquisition of information is legal or not, the act of placing it in a malicious abuse scenario and completely subverting the original privacy boundary itself constitutes a substantial infringement upon the sensitivity of the information. Their purposes are mostly aimed at fraud, defamation, etc., lacking the support of common interests. Moreover, through technical means, information is infinitely copied and tampered with, overstepping the scope of privacy interest retention and magnifying the risk of infringement. Deepfakes conduct in-depth analysis of biometric features. Once the information is used for false content outside the initial context, it poses a direct threat to personal dignity and property safety. The malicious transformation of the context itself constitutes an endogenous high risk.

Therefore, the fundamental harm of deepfake behavior lies in the qualitative change of risks caused by the alteration of scenarios. Regardless of whether the source of the information is legal or not, deviating from the initial scene and purpose constitutes a substantive infringement upon sensitive personal information. The focus of legal protection should shift from the formal review in the data acquisition stage to the substantive assessment of the usage scenarios, and based on this, confirm its criminal punishable nature.

DOI: 10.54254/2753-7048/2026.32781

3.2. Illegal determination of processing citizens' personal information by using deepfake technology

3.2.1. The illegal determination of deepfake behavior is divided

Legislative proponents argue that traditional post-event punishment is difficult to deal with the characteristics of deepfakes, such as their infinite continuation, uncontrollable spread and exponential growth in harm on the Internet. It is necessary to strengthen the preventive function and promote the "front-end extension" of regulation. The specific approach includes adding the crime of "identity fraud" to fill the gap of pure identity fraud without identification documents, without targeting specific groups, and without subsequent crimes [14]. Or introduce the "crime of identity theft", arguing that the current evaluation only indirectly restricts upstream and downstream crimes, and there are gaps in key links such as the independent harmfulness of deepfakes and illegal use after legal acquisition. It is necessary to establish a tiered and intensified protection system for personal information [15]. However, this position requires a response: Is there indeed no room for explanation for the existing charges? Is the legislative path of integrated online and offline regulation lacking judicial feasibility? Does identity-related crimes have the connotation of independent infringement of legal interests? Opponents, however, argue that the essence of the risk of deepfakes lies in the intensification or compounding of the existing legal interests rather than the infringement of new legal interests. Therefore, specialized legislation lacks legitimacy and necessity, and responses should be made through judicial approaches such as lowering the threshold for crimes and increasing the severity of penalties [16]. However, it is also necessary to further clarify: Is it reasonable to simply attribute the compound of legal interests to "quantitative increase"? Could the features of new technologies possibly give rise to infringements on new legal interests such as digital identities? Accordingly, for the determination of the illegality of processing citizens' personal information through deepfake technology, two prerequisites must first be clarified: Does the act of deepfake itself have an independent illegal connotation that requires special evaluation by criminal law? Is it sufficient to be an independent object of criminal law liability?

3.2.2. Legal interest correction for deepfake behavior

Deepfake technology not only infringes upon the "information" itself, but also the "digital identity" system constructed by the information and featuring social functions. Digital identity is a trinity identity system formed by integrating information such as biological characteristics, social relationships, and behavioral trajectories. Its core lies in the unification of the unified identification of digital individuals and their social credibility [17]. The unique harm of deepfakes lies in the following: First, by forging biometric features, it directly undermines an individual's "unique identity" in the digital space and destroys the ontological foundation of identity identity. Secondly, by generating false identity authentication certificates, individuals are deprived of control over their digital identities. Thirdly, by forging behavioral data and fabricating social relationships, the social credibility on which digital identities rely for survival is polluted. This act itself has been transformed through the attribute of legal interest and predestined for potential damage, constituting an independent unlawful consequence.

DOI: 10.54254/2753-7048/2026.32781

3.2.3. The justification of legal interests protected by digital identity in criminal law

The information revolution has driven the deep integration of digital technology and the real society, giving rise to an infinitely extended virtual space beyond the traditional physical space, thereby building a two-layer social structure that is isomorphic between the virtual and the real [18]. Individual information is decomposed and integrated into a recognizable digital identity. The identification method has evolved from the simple authentication of the initial combination of username and password to the centralized authentication of multi-factor and integrated identity management, and then transformed into decentralized authentication represented by blockchain technology and smart contracts [19]. Although decentralized digital identity recognition has significant advantages such as autonomy, controllability, and tamperability, it has also triggered new risks such as privacy leakage, identity theft, and legal regulatory predicaments. The cybersecurity situation demands the construction of a trusted digital space. Digital identities have become an important strategic infrastructure project for ensuring cybersecurity, supporting the digital economy, and promoting the modernization of national governance capabilities [20]. Digital identities not only carry personal interests but also have attached interests and transaction functions [21]. Although their rights and interests belong to individuals, the infringement of digital identities will simultaneously undermine the social trust mechanism and information order [22]. Therefore, the regulation of criminal law should take into account the rights and interests of individuals' identities and the stability of the social system and other transpersonal legal interests, to achieve the dual goals of the rule of law.

4. The path to improving criminal law regulation on the abuse of deepfake technology

4.1. Attempts to commit the crime of infringing upon citizens' personal information

The interpretation of criminal law should adhere to the approach of substantive and standardized thinking [23]. The crime of infringing upon citizens' personal information is based on the premise of "violating relevant state regulations". The Civil Code and the Personal Information Protection Law provide guidance on the criteria for conviction. Accordingly, personal information processors may process personal information that has not been illegally disclosed within a reasonable scope, except where the individual explicitly refuses or fails to obtain the individual's consent, thereby causing significant impact on the individual's rights and interests. Where the purpose, method or type of personal information processed changes, the individual's consent shall be obtained again. Therefore, the protection of personal information should follow the standards of purposefulness. The purpose for which an individual discloses their information and the use of the information are part of the legal interest. If processing personal information obviously violates the purpose for which the individual discloses it or changes the use of the disclosed information, it may constitute this crime [24]. For the act of abusing deepfake technology, if the perpetrator uses personal sensitive information for illegal and criminal activities, it has obviously violated the expected purpose and use of the right holder, and may infringe upon legal interests, constituting the ground for conviction of the crime of infringing upon citizens' personal information.

DOI: 10.54254/2753-7048/2026.32781

4.2. Give full play to the role of filling the gap in the crime of illegally using information networks

In response to the act of processing personal information through deepfake technology, criminal law should prioritize the interpretation theory over the legislative theory for system optimization, precisely targeting the "act of release" as the object of responsibility, and relying on existing criminal charges to achieve effective regulation. The cost of adding new crimes is high and it involves a large amount of judicial interpretation coordination and system integration. However, the interpretation theory has a lower cost and is more conducive to maintaining the stability of criminal law. Therefore, any goal that can be achieved through the interpretation theory should not be easily turned to the legislative theory [25].

In practice, many cybercrimes can only have their online behaviors identified, while the offline harms are difficult to be fully investigated [26]. However, the act of forging information release has the characteristic of "accumulating to constitute a crime". The harm caused by a single act is limited, but with the help of network technology, it can be repeated in large quantities, and the cumulative harm can reach the level of criminal penalty. This behavior creates conditions for back-end crimes, exists independently and plays a key role in the industrial chain. It should be granted an independent criminal status to achieve "early detection and early intervention" and cut off the black industrial chain. The production and release of deepfake information are entirely dependent on network tools, which aligns with the technical dependence, heterogeneous harmful consequences, and media-like characteristics of network tool-type crimes. The crime of illegally using information networks, by criminalizing some acts with preparatory nature independently, is an inevitable choice to deal with the virtual nature of the network risk society, the transcendence of technology and the involvement of the order of the masses [27].

In terms of specific application, a hierarchical view of legal interests should be adhered to, and a two-tier structure of "blocking layer legal interests" and "backing layer legal interests" should be adopted to clearly define the criteria for criminal and illegal activities, the logic for judging serious circumstances, and the application direction of competitive and cooperative clauses [28]. If the downstream behavior of deepfake constitutes a criminal act as stipulated in the specific provisions of the Criminal Law, it will inevitably cause a double risk to legal interests, and this crime shall be applied. If the downstream behavior is an illegal act stipulated in the specific provisions of the Criminal Law but does not constitute a crime, the degree of infringement of the legal interests of the blocking layer is quantified through "serious circumstances". If the abstract danger reaches the level of a crime, this crime shall be applied. In terms of the application of the concurrent provision, if the illegal act of releasing deepfake information "simultaneously" constitutes a downstream criminal act, causing specific danger or real harm, and the punishment for the downstream crime is concurrent with the third item of the first paragraph of the crime of illegally using information networks, which states "releasing information for the purpose of carrying out fraud and other illegal and criminal activities", the more severe punishment should be chosen.

4.3. Construction of a collaborative mechanism for network service providers

The discussion on the illegality of deepfake information begins with the public release and dissemination, and so does the criminal obligation and responsibility of network service providers. Its criminal responsibility, as an indirect liability, is premised on the typification of network service providers and based on the precise definition of criminal obligations.

DOI: 10.54254/2753-7048/2026.32781

From the perspective of comprehensive classification, based mainly on service type standards, supplemented by service objects and methods, network content service providers and network intermediate service providers are distinguished. The latter includes network intervention service providers, network information location service providers, network storage service providers and network platform service providers [29]. The scientific nature of this classification lies in achieving a precise correspondence between responsibilities and obligations. For instance, a network service provider could be a content service provider itself, which voluntarily posts deeply forged obscene videos on self-built video websites and thereby bears the responsibility of a principal offender or an accomplice. In the modern online ecosystem, the criminal obligations of different types of service providers have their own emphases, mainly including content management obligations, security protection obligations, and regulatory cooperation obligations [30]. Content management obligations mainly include the obligation of pre-review, real-time monitoring and notification of deletion. If users voluntarily evade review and spread illegal information under real-name supervision, such intervention may cut off the direct causal chain of the platform, making their actions less likely to lead to serious consequences. At this point, the violation of obligations may not escalate to criminal responsibility [31]. Deepfake platforms with a large amount of data may become information repositories illegally obtained by individuals. According to Article 42 of the Cybersecurity Law, operators of deepfake platforms shall take technical measures and other necessary measures to ensure the security of the personal information they collect, prevent the leakage, damage or loss of information, and thereby bear the obligation of information security.

The safe harbor principle is the main basis for network service providers to supervise the exemption of liability for negligence, aiming to balance information security and information freedom [32]. However, the connotation of the obligation of information network security management should also include enhancing the security of network operation and proactively preventing online criminal activities. The safe harbor system should not be a reason for neglecting to fulfill the obligation of network security supervision. Network service providers should not mechanically execute the "notice-and-delete" procedure. Instead, they should enhance their duty of care after deletion and take technical measures to prevent the repeated upload of similar infringing content.

In addition, when evaluating the illegality of the actions of network service providers, an overall consideration is required. Although it has intervened to some extent in the dissemination of illegal information, it is also committed to providing a relatively neutral platform for various types of data, merely because the indirect profit model objectively promotes the circulation of deepfake information. Therefore, it is advisable to appropriately break through the strict technical neutrality stance and instead comprehensively determine the criminal illegality and degree of their actions in combination with the consistency of their commercial intentions, technical behavior patterns, and social harmful consequences.

5. Conclusion

The emergence and abuse of deepfake technology is one of the microcosm of technological risk governance in the era of artificial intelligence. The core of governance lies in the innovation of thinking and paradigms, and the ultimate goal is to achieve a dynamic balance [33]. It is necessary to avoid both the stifling of technological innovation due to excessive criminal regulation and the indulgence of technological abuse due to insufficient regulation, which could lead to a crisis of social order and trust. We should abandon the rigid regulatory approach of simple blocking and instead build a set of rules that are both adaptable and operational to flexibly deal with similar

DOI: 10.54254/2753-7048/2026.32781

technical challenges that may arise in the future. Only in this way can we manage risks while ensuring the healthy and orderly development of technology.

References

[1] Cao, J.F. (2019) The Legal Challenges and Responses to Deepfake Technology. Information Security andCommunication Privacy, 10, 35–40.
[2] Wang, L.S. (2019) Integrated Regulation of "Deepfake" Intelligent Technology. Oriental Law, 6, 58–68.
[3] Zhang, H. (2020) Threats and Governance of "Deepfake" in Cyberspace. Cyberspace Security, 5, 45–51.
[4] Huang, J., Han, S.Y. and Tian, Y.H. (2025) Pattern Characteristics, Generation Logic, and Regulatory Strategies ofDeepfake Risks in Generative Artificial Intelligence. E-Government, 5, 31–41.
[5] Wu, J.E. and Feng, S.C. (2023) The Impact of "Deepfake" Technology on Judicial Cognition and ItsCountermeasures. Learning and Exploration, 9, 67–76.
[6] Liu, X.Q. (2025) Criminal Law Regulation of Deepfake Behavior in the Era of Artificial Intelligence. Politics andLaw, 11, 48–61.
[7] Yang, J.W. and Luo, F.Y. (2025) Hierarchical and Classified Management: Content Risks and Legal Regulation ofGenerative Artificial Intelligence. Journal of Kunming University of Science and Technology (Social SciencesEdition), 6, 13–22.
[8] Bao, Y.X., Lu, T.L. and Du, Y.H. (2020) A Review of Deepfake Video Detection Technology. Computer Science, 9, 283–292.
[9] Du, J.W. and Pi, Y. (2022) International Perspectives and China's Position on Criminal Law Protection ofBiometric Information in the AI Era: Starting from the Misuse of Information under "Face RecognitionTechnology". Hebei Law Science, 1, 144–167.
[10] Zheng, G.J. (2025) Criminal Law Response to the Abuse of Deepfake Technology. Science of Law (Journal ofNorthwest University of Political Science and Law), 3, 56–68.
[11] Fan, W. (2016) Reconstructing the Path of Personal Information Protection in the Big Data Era. Global LawReview, 5, 92–115.
[12] Yang, X. and Xu, Z.H. (2025) Criminal and Civil Distinction of the Infringement of Sensitive Personal Informationunder Scenario Theory. Economic Criminal Law, 1, 343–368.
[13] Ji, L.L. (2022) Judicial Dilemmas in Defining Private Information and Solutions. Journal of Shanghai University(Social Sciences Edition), 6, 94–108.
[14] Li, T. (2020) Construction of a Criminal Law Regulation System for "Deepfake" Technology. Academic Journal ofZhongzhou, 10, 53–62.
[15] Li, H.S. (2020) Criminal Sanctions for Misuse of Personal Biometric Information: Taking AI "Deepfake" as anExample. Tribunal of Political Science and Law, 4, 144–154.
[16] Jiang, Y. (2021) The Direction and Limits of Criminal Law Regulation of AI "Deepfake" Technology Risks. SocialSciences in Nanjing, 9, 101–109.
[17] Li, X.J. (2024) The Technological Power and Regulation of Digital Personal Identity Authentication. China LegalScience, 1, 145–165; Zhang, C. and Lyu, K. (2022) Research on Personal Identity Authentication in the Era ofArtificial Intelligence. Journal of Hefei University of Technology (Social Sciences Edition), 2, 23–34.
[18] Ma, C.S. (2018) Legal Changes in the Age of Intelligent Internet. Legal Research, 4, 20–38.
[19] Jin, M.G. (2024) Legal Risks of Digital Identity Recognition in the Context of Decentralization andCountermeasures. Journal of Sichuan Normal University (Social Sciences Edition), 5, 69–79.
[20] Yu, R. (2022) Digital Identity Construction in Various Countries and China's Trusted Digital Identity DevelopmentPath. Information Security Research, 9, 858–862.
[21] Chen, L. (2025) Justification of Legal Interests in Criminal Law Protection of Digital Identity. Economic CriminalLaw, 1, 319–342.
[22] Guo, J.P. (2023) Criminal Law Regulation of Identity Theft in the Era of Artificial Intelligence. Journal ofGuangzhou Public Security Management Cadre College, 3, 31–37.
[23] Zhou, G.Q. (2021) Practical Application of the Principle of Unity of Legal Order. Rule of Law Society, 4, 1–12.
[24] Zhou, G.Q. (2021) The Object of Conduct in the Crime of Infringing on Citizens' Personal Information. TsinghuaLaw Review, 3, 25–40.
[25] Liu, Y.H. and Jiang, W.Z. (2024) Correction of Criminal Law Regulation of AI Face-Swapping: A Dual Path ofLegal Interest and Number of Crimes. Journal of University of Chinese Academy of Social Sciences, 5, 5–30.
[26] Yu, H.S. (2016) Legislative Expansion and Judicial Application of Cybercrime. Legal Application, 9, 2–10.

DOI: 10.54254/2753-7048/2026.32781

[27] Chen, W. and Xiong, B. (2020) The Characteristics and Legislative Techniques of Cybercrime: An InvestigationBased on the "Dual-Layer Society" Pattern. Journal of Dalian University of Technology (Social Sciences Edition), 2, 63–70.
[28] Wang, G.Z. (2023) Identification of Legal Interests and Application Direction of the Crime of Illegal Use ofInformation Networks. Academia, 7, 138–151.
[29] Yang, C.X. (2018) Typified Reflection on the Criminal Responsibility of Network Service Providers. Legal Science, 4, 162–172.
[30] Shi, Q.W. (2023) Typified Research on Criminal Responsibility of Network Service Providers. Criminal LawReview, 3, 27–48.
[31] Chen, X.L. (2006) From Attribution to Imputation: Research on the Theory of Objective Imputation. LegalResearch, 2, 70–86.
[32] Li, M.L. (2021) Criminal Law Governance Path for "Deepfake". Science Technology and Law (Chinese-EnglishEdition), 6, 40–47.
[33] Cai, S.L. (2020) The Technological Logic and Legal Transformation of "Deepfake". Political Science and LawTribune, 3, 131–140.