The Infringement of Deepfake Technology on Personal Privacy and Legal Protection: A Discussion Based on Article 1032 of the Civil Code

Mengqi Han *

Department of Law and Politics, North China Electric Power University， Baoding, China

* Corresponding Author Email: bdzsb@ncepu.edu.cn

Abstract. The rapid development of deepfake technology has infringed upon personal privacy in the form of the disclosure and misuse of personal information, infringement upon the peace of people's life, and damage to personal image and reputation. The disclosure and misuse of personal information should be analysed from the perspectives of personal use and commercial use of information data; infringement upon the peace of people's life should be examined from the perspectives of fraud and harassment, and malicious pursuit using deepfake technology; and damage to personal image and reputation should be discussed from the two levels of initial damage to personal image and reputation and aggravated damage to personal reputation after dissemination through the media. Article 1032 of the Civil Code clearly defines the scope of privacy protection as the peace of people's private life, private space, private activities and private information, as well as the infringement of privacy rights through means such as spying, intrusion, disclosure and publication, which reflects the legislative inertia to strengthen the protection of privacy and personal information. Article 1032 of the Civil Code, the Personal Information Protection Law, the Provisions on the Administration of Deep Synthesis of Internet-based Information Services, and other laws and regulations together form the current personal privacy protection system. However, existing laws do not provide specific explanations for key terms such as 'leakage', 'intrusion' and 'damage', which leads to uncertainty in the application of the law and makes it difficult to effectively protect personal privacy in actual operations. At the same time, there is a lack of clear definitions of the scenarios and specific standards of behaviour that the technology may involve, which has exacerbated public concerns about personal privacy security. Strengthening legal protection against deepfake technology requires refining legal concepts and drawing on knowledge from comparative law: 'leakage' can be considered the illegal acquisition and dissemination of unauthorised data and information, 'intrusion' can be defined as behaviour that disrupts the normal order of others and causes mental distress, and 'damage' can be understood as behaviour that causes negative evaluation or loss to the image, reputation or property of others. The legislative department should take the lead and cooperate with the Ministry of Industry and Information Technology in formulating specific standards for evaluating behaviour. The deterrent effect of the law should be strengthened by refining relevant legal provisions in the Civil Code and the Personal Information Protection Law and increasing the penalties for violations of the law. This will better balance technological development and personal privacy protection and improve China's personal privacy protection system.

Keywords: Eepfakes, personal privacy, personal information, infringement, legal protection.

1. Introduction

1.1. Research Background

The convenience of deepfake technology has made image and video editing and tampering easier, but it has also brought about problems of privacy leakages and abuse. For example, AI face-swapping apps excessively collect personal information and are even used to create fake videos and images to defraud and slander others. These fake information spreads on the Internet and is difficult to eliminate, which seriously damaging the reputation and rights of the victim. The infringement of personal privacy is not only an issue of individual rights, but also relates to national security and social stability. Therefore, attention must be paid and measures must be taken to regulate the use of deepfake

technology. With regard to the excessive collection of personal information by apps[1], supervision should be strengthened to prevent the abuse of user data. Meanwhile, lawbreakers who use deepfake technology to commit malicious acts should be punished to maintain social order and public interest. In addition, the public's ability to identify fake information should be improved to reduce its spread and impact.

1.2. Significance of the Research

1.2.1. Theoretical Significance

Promote the convergence and coordination of laws and regulations related to deepfake technology both internally and externally. The simplicity, novelty， and technological nature of deepfake technology determine that systematic institutional arrangements must be made when it is associated with legal protection issues, so that different laws have different regulatory objects and protection methods for the regulation of face recognition. However, the construction of a systematic and effective legal protection system needs to take the opportunity of comprehensive legislation such as the Civil Code, the Personal Information Protection Law, and the Provisions on the Administration of Deep Synthesis of Internet-based Information Services, focusing on discussing the provisions of Article 1032 of the Civil Code on the right to personal privacy, to construct a jurisprudence for deep counterfeiting, to give full play to the functions of various depatment laws in protecting rights and ensuring security, to achieve a benign interaction between administrative legislation and criminal law norms, to promote the substantiation of criminal law norms, and to improve the internal and external convergence and coordination of laws and regulations for deep counterfeiting technology.

1.2.2. Practical Significance

At the practical level, the significance of this research is mainly reflected in the following aspects. First, it provides practical guidance for the protection of personal privacy. By analysing deepfake technology, we can understand its operating principles and potential risks, thereby providing individuals with effective preventive measures and response strategies. At the same time, this article will combine the provisions of Article 1032 of the Civil Code to provide specific guidance for individuals on how to safeguard their rights according to law when facing infringement of privacy. Second, it provides a reference for the improvement of relevant laws and regulations. As deepfake technology continues to develop, the relevant laws and regulations also need to be constantly updated and improved. By studying deepfake technology and its impact on personal privacy, valuable reference can be provided for national legislative and judicial authorities to promote the improvement and revision of relevant laws and regulations. Third, it promotes the benign development of information technology. By regulating and standardising deepfake technology, it can guide the development of information technology in a more positive and more sustainable direction.[2] Additionally, this study will explore how to protect personal privacy while giving full play to the positive role of deepfake technology and provide impetus for social development.

2. Deepfake Technology Infringes On Personal Privacy

2.1. Leakage and Abuse of Personal Information

With the development of deepfake technology, the theft of personal information has become increasingly rampant, which has become a serious challenge that threatens personal privacy. Using highly realistic video and audio as tools, this type of technology can easily impersonate individuals and infiltrate into fields such as finance and social media to steal identity information and sensitive data. In order to protect the security of personal information, it is necessary to strengthen technical supervision and enhance public discernment. According to Article 1032 of the Civil Code[3], natural persons have the right to privacy and the right to information self-determination with respect to their personal information. Any organisation or individual processing the private information of another person without consent constitutes infringement. [4] However, deepfake technology not only creates

visual illusions, but can also steal personal information without the user noticing. In addition, commercial organisations may use this technology to conduct illegal commercial promotional activities, which seriously infringes on privacy rights, the right to information self-determination, and disrupts the market order. [5] Therefore, effective measures must be taken to prevent such risks, protect personal privacy rights, maintain market order and safeguard the public interest.

2.2. Violation of Personal Peace

With the popularisation of deep fake technology, ordinary people can easily create personal virtual profiles and commit fraud. Criminals use synthetic speech, artificial intelligence face replacement, and other methods to screen out gullible people for targeted scams, making this form of crime highly covert and deceptive. For instance, in a 2023 case from the Baotou Municipal Public Security Bureau, criminals used deep fake technology to deeply learn image and audio information to commit video call scams. [7] By obtaining the private information of others, perpetrators or commercial organisations use this information to blackmails, make improper threats, maliciously slander, etc., which causes great harm to the victim's reputation and privacy. [8] To prevent this kind of incidents, it is necessary to strengthen awareness of network security, strictly control the leakage of personal information, and enhance law enforcement.

2.3. Damage to Personal Image and Reputation

Deepfake technology can easily tamper with people's image and damage their reputation through highly realistic image, audio or video synthesis. This negative impact may cause the infringed person to lose trust in society and affect their normal life and work. Once deepfake content is widely spread through channels such as social media and news websites, it will not only exacerbate the severity of the original infringement, but also further undermine the victim's social evaluation and personal dignity, creating a vicious cycle. There are three reasons for these negative consequences. First, in an Internet context, personal privacy will completely lose its natural barriers such as space and activities, making it difficult for individuals to protect their privacy interests through traditional physical space facilities such as residences. Second, due to the fast speed, wide range, and long duration of the dissemination of digital information, when individual information is tampered with in the digital space by deepfake technology, it will have a significant impact on the individual's normal life and work. Third, from the perspective of technological development, the application of deepfake technology in Internet information services still lacks an effective technical review mechanism,[10] which leaves relevant staff and departments without technical support when reviewing, disseminating, and evaluating fake videos. As a result, personal privacy rights are facing unprecedented challenges in the digital space.

3. Analysis of the Current Legal Protection Situation Based on Article 1032 of the Civil Code

When discussing the infringement of personal privacy rights by deepfake technology and legal protection, Article 1032 of the Civil Code, the core provision on privacy protection, should be thorougly analyzed.

3.1. Interpretation of Article 1032 of the Civil Code

3.1.1. Scope of Protection of Privacy

Article 1032 of the Civil Code stipulates'Natural persons shall have the right to privacy. No organisation or individual shall infringe upon the right to privacy of another person by means of probing, intrusion, disclosure or publication.' Among these, 'spying' refers to the act of obtaining another person's biological information or other personal private information without their consent; 'intrusion' refers to the illegal interference with or infringement of another person's private space or private activities; 'disclosure' includes both active and passive forms of disclosure, that is, whether

the private information is improperly obtained or disseminated through active behaviour or negligence; and 'publicity' is when such private information is made public by an unauthorised third party. This provision first clarifies the scope of protection of privacy rights, including but not limited to the private life and peace of mind of natural persons and private spaces, private activities, and private information that they do not want others to know. [11] This definition not only covers privacy in the traditional sense of physical space, such as protection against illegal intrusion into a home, but also extends to privacy in cyberspace in the information age, such as sensitive personal data such as portraits, voices, and identity information, as well as records of online activities. Against the backdrop of increasingly rampant deepfake technology, the breadth of this scope of protection is particularly important, as it ensures that an individual's privacy in the digital world is also strictly protected by law.

Although there is a legal difference between privacy protection and personal information protection, they are often confused. Privacy is considered a more central right, while personal information is considered an interest. Nevertheless, the legal protection of personal information is stricter. From an individual perspective, privacy is protected in most cases before personal information. Personal information involves a wide range of groups, and the law requires a higher degree of prevention. [12] With regard to the principle of compensation for damages, the privacy protection protects equal individual relationships and adopts the principle of fault; while the protection of personal information requires the correction of unequal information capabilities and adopts the principle of presumed fault or illegality to promote compliance in information processing.

3.1.2. Fundamental principles of tort liability

Article 1032 of the Civil Code establishes the basic principle of tort liability, i.e., no organisation or individual may infringe upon another person's right to privacy by spying, intruding, divulging, disclosing, etc. This principle provides a clear legal standard for determining whether deepfake constitutes infringement. Meanwhile, Article 1167 of the Tort Liability Law stipulates that where a tort endangers the personal or property safety of another person, the victim of the tort may require the tortfeasor to assume the tort liabilities including but not limited to cessation of infringement, removal of obstruction and elimination of danger.

According to Articles 179 and 995 of the Civil Code, the ways in which the perpetrator bears tort liabilities include but not limited to cessation of infringement, removal of obstruction and elimination of danger, elimination of the impact, restoration the reputation, apologies and making compensation for losses, etc., providing the victim with comprehensive legal remedies.

3.2. Deepfake and the Applicability of Article 1032 of the Civil Code

In the Civil Code, Article 1032 is a provision on the protection of personal privacy. This article clearly states that every natural person has the right to privacy, regardless of individual status, and there are no differences due to factors such as nationality or age. This right is one of the basic rights of the person and is highly protected by law. With the continuous development of deep forgery technology, the infringement of personal privacy rights is becoming more and more serious. Article 1032 of the Civil Code is an important legal basis for the protection of privacy rights, and its applicability has become the focus of atattentio.

3.2.1. Does Deepfaking Constitute a Violation of Privacy?

First, there are cases where it does. Deepfaking in the context of privacy involves the unauthorised alteration, processing or fabrication of personal images, videos and audio messages and their publication. This constitutes a serious violation of privacy. It should be noted that speech and actions in public places are not considered private and are therefore not subject to this restriction. However, even if deepfake creations are made within legal limits, if the results have a negative impact on the reputation and image of the subject, it should also bear corresponding legal responsibility. If personal private information, portraits, voices, etc. are deepfaked without authorisation and made public or used for other improper purposes, this constitutes an infringement of privacy and requires additional

protection. [13] Therefore, when using this technology, the basic principle is to respect privacy and maintain reputation.

Second, there are situations that do not constitute an infringement of privacy. The first one can be deepfakes involving public interest. In specific situations, when important issues such as public safety and social governance are involved, the government or relevant institutions may use deepfakes to create simulated images or videos. If these simulated information does not cause substantial harm to personal privacy and is used within the scope permitted by law, then this behavior does not constitute an infringement of privacy. The second is deepfakes involving harmless expression. If individuals or organisations use deepfakes for harmless self-expression or entertainment and do not substantively affect the privacy of others, then such behaviour does not require special protection and should not be punished. [14] For example, non-profit, non-harmful images and videos of friends made using each other' s portraits can be considered normal forms of communicative expression.

3.2.2. Identification of Legal Liability and Its Difficulties

According to Article 1165 of the Tort Liability Law, infringement of privacy rights requires the fulfilment of four elements: subjective fault, damage, illegality and causality. Specifically, the perpetrator must act with intent; there must be facts of damage such as personal information being illegally obtained, tampered with or improperly used; the focus is on illegal acts such as unauthorized photography, recording or use; and the illegal act must directly lead to infringement of privacy rights in order to be considered infringement. These four elements collectively form the framework for determining liability in privacy infringement cases.

Based on the characteristics of deepfake technology and the principles of infringement, the process of deepfake technology infringing on privacy is divided into three stages.The first stage involves the acquisition of another individual's biometric data to meet the needs of deepfake creation (e.g., face-swapping, voice-modification), often accompanied by 'spying' or 'intrusion' into personal privacy. The second stage involves the use of deepfake technology to perform face or voice replacement, achieving a realistic effect. This stage completes the substitution of personal information. The third stage is the unauthorised and illegal disclosure of such information or other acts that infringe upon the privacy of others. This stage is where the privacy right actually suffers damage. However, in determining tort liability, two main challenges arise:

In the first stage, there are difficulties in determining the act of 'spying'. Due to the hidden nature of deepfake technology, 'spying' is often difficult to detect and identify, which makes it difficult to stop the infringement in a timely manner. In the third stage, i.e. the unauthorised and illegal disclosure of personal information, is reflected in three aspects. First, the difficulty in identifying the perpetrator. Due to the anonymity and concealment of deepfake technology, it is hard to determine who committed the act of disclosure, making it difficult to hold the offender accountable for the infringement. Second, the difficulty in assessing the extent of the damage. Even if the perpetrator can be identified, determining the extent of harm caused to the victim by the act of disclosure remains a challenge, requiring the assessment and judgment of professional legal and technical teams. Third, it is difficult to protect the privacy of ordinary people in a timely and effective manner. Due to the difference in popularity, the difficulty and effectiveness of protecting the privacy of ordinary people and celebrities are different. The privacy of ordinary people is often difficult to protect in a timely and effective manner, while the privacy of celebrities may be more easily discovered and exploited due to their public attention. [16] Therefore, in terms of legal protection, more attention should be paid to the protection of the privacy rights of ordinary people in order to achieve the principle of equality before the law.

4. Comparison of the Current Status of Relevant Domestic and Foreign Legal Protection and Comparative Analyses

With the rapid development of artificial intelligence technology, deepfake technology has brought convenience while also raising the serious problem of personal privacy infringement. To address this challenge, a series of laws and regulations have been initially established at home and abroad.

4.1. Analysis of the Current Status of Relevant Legislation At Home and Abroad

From the perspective of domestic laws and regulations related to deepfake technology, in addition to the personality rights chapter of the Civil Code, which clearly protects personality rights such as portrait rights, reputation rights, and privacy rights, and Article 1019, which emphasises that acts that infringe upon the rights of others by means of information technology such as deepfake technology shall be subject to legal sanctions, China has also introduced a series of laws and regulations related to network security and personal information protection, such as the Personal Information Protection Law, the Network Security Law, and the Regulations on the Management of Online Audio-Video Information Services. These laws and regulations also provide a legal basis for regulating deepfake technology.

The Personal Information Protection Act is pivotal in protecting the security of personal information. The Act establishes, in principle, the right of individuals to be informed of the handling of their information, and details specific requirements for informing and providing information. Individuals enjoy the right to make decisions, the right to restrict processing and the right of refusal, and may decide on their own how their information is to be processed. In addition, individuals have the right to inspect and copy personal information, and the right to request that inaccurate or incomplete personal information be corrected and supplemented. Individuals may also have their information transferred to a personal information processor of their choice when the prescribed conditions are met. When legal circumstances exist with respect to personal information, the processor is required to voluntarily delete the information. At the same time, individuals have the right to request an explanation of the rules governing the handling of personal information. These provisions constitute a comprehensive and detailed framework to ensure the lawful and safe handling of personal information and provide solid legal protection for the protection of personal information in the online environment [17].

The European Union has incorporated deepfake technology into the General Data Protection Regulation (GDPR), which protects individual privacy through a data governance and numeracy law model of regulation, and imposes strict rules on personal information protection [18]. Although similar to the Personal Information Protection Act, it differs in some key aspects. First, the right to erasure in the GDPR covers the right to be forgotten, which is not addressed in domestic law. Second, the right to make decisions and request explanations, which are specific to the Personal Information Protection Act, are not explicitly defined as universal rights in the GDPR, although its Article 22 has similar requirements for automated processing practices. Both emphasise the data subject's rights to information, access, rectification and supplementation, and restriction of processing, but there may be differences in implementation details and applicable contexts. In addition, the right to portability is a GDPR-specific right that allows data subjects to access structured personal data from data controllers in specific circumstances. The differences in these rights reflect the different emphases and considerations of different legal systems with respect to the protection of personal data. Therefore, a combination of country-specific provisions and practicalities need to be taken into account when interpreting and implementing these laws.

4.2. Comparative Analysis of Domestic and Foreign Legal Practice

In terms of legal practice, domestic and foreign countries also show different characteristics.

Firstly, the legislative modes are different. China prefers to regulate deepfake technology through a comprehensive system of laws and regulations, focusing on the construction of legal frameworks

from multiple perspectives, such as the protection of personality rights and the protection of personal information. While foreign countries are more likely to adopt special legislation or amend existing laws to formulate special legal provisions for the characteristics of deepfake technology, such as the U.S. State of Texas, "Biometric Information Access and Use Act" in accordance with the process of information collection, use stage regulation; Washington State, "Washington Privacy Act" specifies the data rights subject of the personal information of the rights of the rights of the subject, such as the right of access, the right to correction, the right to delete, etc. [20] Provisions are made to respond to infringement in a more direct and effective manner.

Second, the difference in legal enforcement efforts. Domestic law enforcement efforts in cases of infringement of deepfake technology have been continuously strengthened, and the relevant legal provisions have been continuously improved through judicial practice to enhance the accuracy and effectiveness of the application of the law. Articles 20 to 22 of the Tort Liability Law provide for compensation for property or mental damage caused by infringing on the personal rights and interests of others, while Article 66 of the Personal Information Protection Law also specifies that offenders shall be fined to varying degrees according to the severity of the circumstances, in order to safeguard the legitimate rights and interests of the victims. In foreign countries, especially in the European Union, its General Data Protection Regulation has higher regulations and penalties for deepfake. According to Article 83 of the Regulation, the corresponding subjects are held liable according to different infringement situations. In addition, the Regulation also provides for fairly high administrative fines, which can be equal to 2 per cent or 4 per cent of a company's total global turnover for the previous year, whichever is higher [21]. Thus, it can be seen that China's law enforcement efforts in cases of infringement of deepfake technology is being strengthened, but compared with the EU's General Data Protection Regulation, its regulation and punishment still need to be improved.

Thirdly, the timing of intervention is different. In combating deepfakes, China often relies on the investigation of public security organs and trials by judicial organs afterwards, such as the "Tort Liability Law" article 36 of the infringement of the infringement of the aftermath of the occurrence of the regulation. While foreign countries pay more attention to technical prevention and pre-regulation, through the establishment of sound technical monitoring and early warning mechanism [22]. For example, the U.S. House of Representatives proposed the Deep Fake Liability Act, which requires that anyone who creates a deep fake video media file must use "non-removable digital watermarks as well as textual descriptions" [23] to indicate that the media file is tampered with or generated, otherwise it will be a criminal offence.

In conclusion, the legal protection of technical characteristics in the EU and the United States is comprehensive and precise. First of all, special legal provisions provide a strong guarantee for the protection of the rights and interests of citizens. In addition, in terms of legal accountability, the strict and meticulous attitude makes the deterrent effect of the law can be effectively exerted. Lastly, the mature experience of pre-regulation has curbed the phenomenon of in-depth falsification of technology infringement from the source. These international experiences have provided important reference for the improvement of China's legal practice, promoting the synchronisation of law and science and technology, and achieving more comprehensive legal protection.

5. Inadequate Legal Protection Against Deepfake Technology and Suggestions for Improvement

Although Article 1032 of the Civil Code provides general rules on the use of technology, specific legal norms for deepfake technology are still insufficient. Deepfake technology mainly involves three scenarios: personal information disclosure, intrusion of personal peace, and damage to image and reputation. The current law lacks a clear definition of the scenarios and standards of behaviour involved in deepfake technology, and keywords such as 'leakage', 'intrusion' and 'damage' are not specifically explained. In the past two years, regulations such as the Provisions on the Administration of Deep Synthesis of Internet-based Information Services have been introduced to legislate and

regulate specific technical scenarios. [24] However, the stipulation that separate consent is required for the use and editing of facial and voice information. Due to the subjectivity of 'separate consent', there is a lack of objective evaluation criteria. [25] At present, the law's evaluation of deepfake technology mainly relies on subjective judgment and the trial of specific cases, resulting in a high degree of subjectivity and uncertainty in evaluation.

In order to solve the above problems, we need to supplement the interpretation in the law and play the role of the law. First of all, we need to specifically interpret and define key words such as 'leak', 'intrusion' and 'damage'. 'Leak' can be understood as the illegal acquisition and dissemination of unauthorised data and information; 'intrusion' can be understood as behaviour that disrupts the normal order of others and causes mental distress; and 'damage' can be understood as behaviour that causes negative evaluation or loss to the image, reputation or property of others. In the context of the disclosure of personal information, 'leakage' can be understood as the illegal acquisition and dissemination of unauthorised data and information, i.e. deepfake technology may lead to the illegal acquisition and dissemination of personal information or data. Article 111 of the Civil Code also stipulates that no organization or individual may illegally collect, use, process, or transmit other persons' personal information, or illegally sell, buy, provide, or disclose other persons' personal information. Some scholars believe that this is intended to protect and control the dissemination of personal information and shape the 'self-image in the eyes of others'. [26] In the scenario of intrusion of peace, 'intrusion' can be understood as behaviour that disrupts the normal order of others and causes mental distress, i.e. deepfake technology may be used to create false information, causing mental distress to others. As some scholars have argued, the rapid spread of pornographic apps on the internet will have an obvious adverse impact on the social evaluation and normal order of life of victims involved, and will disrupt the peace of them. [27] In the scenario of damage to image reputation, 'damage' can be understood as behaviour that causes negative evaluation or loss to the image, reputation or property of others, i.e. deepfake technology may be used to create fake images or audio, damaging the image and reputation of others. In a tracking report on 'deepfakes', 14,698 'deepfake' videos were displayed online in June and July 2019, an increase of 84% in seven months. The vast majority of these (96%) contain pornographic content featuring women, which seriously damages the image and reputation of women. [28] Another example is the case of a man who used AI technology to fake nearly 7,000 nude photos of his students and colleagues, which seriously infringed on the rights to reputation and privacy of others, damaged the reputation and image of others, not only caused heavy psychological pressure and trauma to the victims, but also had an extremely negative social impact [29].

Furthermore, when formulating specific legal standards and interpretations, the objectivity and generality of the law need to be taken into account. In other words, the legal interpretations and standards should be universally applicable and can be applied to various situations and scenarios. Third, the legal interpretations and standards should have a certain deterrent effect. That is, by clarifying legal responsibilities and penalties, potential lawbreakers will be deterred, and psychological pressure and cost considerations will be brought into play when considering the use of deepfake technology, thus playing a deterrent role and reducing the occurrence of deepfakes.At the same time, it is necessary to consider the cost-benefit relationship, ensuring that the cost of violating the law exceeds the benefits, thereby enhancing the deterrent effect of the law. Lastly, we can also draw on the 'bad guy theory', wherein both legal regulations and the moral responsibility of technology holders collectively contribute to maintaining social order and protecting individual rights [30].

In conclusion, to address the inadequacies in legal protections against deepfake technology, we need to strengthen legal protections by improving laws and regulations, clearly defining the relevant scenarios, establishing specific standards for evaluating behavior, and enhancing the deterrent effect of the law. These efforts are crucial to addressing the challenges posed by modern information technologies and to maintaining the rule of law in society.

6. Conclusion

In the context of rapid technological advancement, this paper discusses deepfake technology and its infringement on personal privacy, with Article 1032 of the Civil Code of China serving as the starting point and central focus of the study.

First, the paper systematically elaborates on three key aspects of deepfake technology's impact: the illegal theft and misuse of personal information, the invasion of personal peace, and the damage to personal image and reputation. Subsequently, it provides a detailed interpretation of Article 1032 of the Civil Code, which clarifies the scope of privacy protection and the fundamental principles of liability for infringement. By comparing the legal protections surrounding deepfake technology in China and abroad, and analyzing them in conjunction with Article 1032, the paper identifies the inadequacies in China's protection of personal privacy rights against deepfake technology. Although certain special laws supplement the general provisions of Article 1032, there is still a lack of objective general evaluation standards and specific behavioral criteria. Terms such as 'disclosure', 'intrusion', and 'damage' are not explicitly defined by the law. Finally, the paper argues for the improvement of the legal system, with the addition of specific provisions and interpretations regarding the behaviors associated with deepfake technology, in order to more effectively safeguard personal privacy rights.

As technology continues to evolve at a rapid pace, deepfake technology presents both challenges and opportunities. Looking ahead, we expect to be able to more accurately assess the potential threat to personal privacy based on an in-depth study of its principles and characteristics. At the same time, we expect to respond to the challenges of emerging technologies by improving the legal system, and strengthen international cooperation and exchanges to jointly promote the development of the legal system. Through continuous research and effort, we believe it is possible to effectively balance technological advancement with the protection of personal privacy, thereby constructing a comprehensive privacy protection system.

References

[1] Yang Junfeng and Zeng Shasha, "Research on the Risks and Countermeasures of the Impact of Deepfake Technology on the News Industry," News World, Vol. 12, No. 13, 2023, p. 13.

[2] Wang Xuan and Song Chunlong, "Research on the Ethical Risks and Regulation Governance of 'Second Creation' Video Based on Deepfake Technology," Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition) 2024, No. 5, pp. 169-170.

[3] Ren Ying, "The Jurisprudential Construction and Rule Remodeling of Privacy Protection in the Digital Era", Oriental Law Journal 2022, No. 2, p. 190.

[4] Cheng Xiao, "The Protection of Privacy and Personal Information in China's Civil Code", in WeChat Public 'Pujiang Law', 08.27.2020.

[5] Ding Xiaodong, "The jurisprudence of the relationship between the protection of privacy and the protection of personal information--Another discussion on the application of the <Civil Code> and the <Personal Information Protection Law>", Law and Business Research, No. 6, 2023, pp. 62-63.

[6] Luo Xin and Zhou Yuan: "The Dissemination Risks of Deefake Technology and Its Governance", Young Reporter, No. 23, 2023, pp. 84-85.

[7] Xinhua: "Internet Association of China: Be alert!" AI face-swapping' new scam', http://www.news.cn/info/20230525/82a2358e05ca4555a0c216a7127ed8f3/c.html.

[8] Xu Qinran, Guo Yibei, et al: 'News Issue 100 | Potential Risks of AI Depth Fake Ads', in WeChat Public 'China-US Legal Review ', 03/23/2024.

[9] Wu Weiguang, 'Understanding the Specificity of China's Privacy Regime from the Generation and Nature of Privacy Interests', Contemporary Law, No. 4, 2017, p. 53.

[10] Shang Haitao, "The New Paradigm and New System of Legal Regulation of 'Deepfake'", Hebei Law Journal, Issue 1, 2023, p. 39.

[11] Wang Liming, "Redefinition of the Concept of Privacy", Jurist, No. 1, 2012.

[12] Peng Chun, "Revisiting the Right to Privacy in Chinese Law and Its Relationship with Personal Information Rights and Interests", Chinese Law Review, Vol. 1, No. 1, 2023, pp. 168-170.

[13] Chen Ran, 'Criminal Laws and Regulations on In-depth Falsification of Sex-Related Information', Jurisprudence 2024, No. 3, pp. 82-83.

[14] Zhang Tao, "The Legal Risks of Deepfake and Its Regulation in the Post-Truth Era," in E-Government 2020, No. 4, pp. 93-94.

[15] Zhu Minming, "The Application Risks of 'AI Face Swap' Technology and Its Regulatory Guidance", in WeChat Public 'Hangzhou Internet Court ', 06/22/2024.

[16] Pan Lu, "Ethical Principles of Celebrity Privacy Concession - From the 'FanCulture'," Young Reporter, No. 14, 2021, p. 105.

[17] Sheng Xiaoping and Tang Yunjie, "Comparative Analysis of China's Personal Information Rights and the EU's Personal Data Rights: Based on the <Personal Information Protection Law> and GDPR," . Library and Intelligence Work, Vol. 6, No. 6, 2022, pp. 27-28.

[18] Li Teng, "The Construction of Criminal Law Regulatory System of 'Deep Forgery' Technology", Zhongzhou Xuekan 2020, No. 10, p. 57.

[19] Wang Xinrui and Luo Wei, "Comparison of the Provisions of the <Personal Information Protection Law> and the GDPR", in WeChat Public ' Net Security Pathfinder ', 09/10/2021.

[20] Bai Shuo and Ji Zekun, "Legal Research on 'Deefake' in the Context of Artificial Intelligence", Modern Marketing (Business Edition), Vol. 11, 2021, p. 127.

[21] Li Huaisheng, "Thoughts on Criminal Sanctions for Misuse of Personal Biometric Information - Taking Artificial Intelligence 'Deep Counterfeiting' as an Example", in Politics and Law Forum 2020, No. 4, pp. 147-148.

[22] Shi Dongxiu, "On the Legal Regulation of Deepfake for Face Swap", Shanghai Law Research Collection, Vol. 5, 2021, pp. 77-78.

[23] "'Face Swap' Crisis: Legal Regulation of Deepfake," in Weixin Public 'Thistle Cybercrime Research', 06/11/2023.

[24] Q&A with reporters on 'Taylor Swift AI Indecent Photos Trigger DEEPFAKE (Deep Fake) Technological Anxiety in the U.S.', Pengpai News.https://www.thepaper.cn/newsDetail_forward_26207479

[25] Wang Liming, 'Fundamental Issues in the Protection of Sensitive Personal Information': with the Interpretation of the <Civil Code> and the <Personal Information Protection Law> as the Background", Contemporary Law, No. 1, 2022, p. 7.

[26] Zhang Wenxian, "Constructing the Legal Order of Intelligent Society", Oriental Jurisprudence, No. 5, 2020, pp. 11-12.

[27] Huang Jiaxing, "The Protection of Personal Privacy in 'Deepfake': Risks and Countermeasures", Journal of East China University of Science and Technology 2022, Issue 1, pp. 129-130.

[28] Kyle Wiggers, "DeepFakes = Counterfeit Maker? An article tells you the current status of deep faking technology", in WeChat Public'AI Data Pie ', Mar. 5, 2020

[29] "Egregious! Man uses AI to forge nearly 7,000 nude photos', https://baijiahao.baidu.com/s?id=1802251950852776934&wfr=spider&for=pc

[30] Zhang Ti, 'Experience and Logic in the Path of Chinese Jurisprudence -The Revelation of Holmes' Argument, Tsinghua Law, 2020, No. 6, p. 8.