DOI: 10.53469/jtpss.2024.04(04).02

Legal Issues and Solutions for AI Face-swapping Technology in the Context of the rule of the Law

Wenyi Yin

Sichuan Normal University, Chengdu, Sichuan, China

Abstract: ***In the context of the rule of law in the new era of network, the protection of personal information rights and interests is an important content of great concern. Through empirical research on the use of AI face-swapping technology, the legal issues in AI face-swapping can be categorized from civil infringement and criminal offense respectively. On this basis, the five aspects of regulating network technology, regulating network platforms, clarifying the main responsibility, improving Blockchain technology, and enhancing citizens' network rule of law literacy can be taken as the "entry point" to regulate the use of AI face-swapping technology, so as to safeguard network security and create a clear cyberspace environment.***

Keywords: Ai face swap; Infringement; Crime; Cyber regulation; Judicial remedies.

1. INTRODUCTION

Technology has a positive effect on promoting economic development and social progress, but on the other hand, it also provides an opportunity to innovate illegal and criminal tools or means, and the legal problems arising from the application of AI face-swapping technology are a typical manifestation of this negative effect. Users through the depth of forgery-related technology to generate a "third person" face for dissemination, will enhance the legal risk of "face" information by the use of lawbreakers. This will not only jeopardize the legitimate rights and interests of the portrait right holders themselves, but also affect the stability of the entire cyberspace, and then disturb the social order. This paper applies the literature analysis method and case study method to analyze and summarize the legal problems caused by AI face-swapping, and puts forward relevant and effective solutions in the context of network development.

2. LEGAL ISSUES IN AI FACE SWAP

The high degree of development of Internet technology has given special value to "faces", which are gradually being digitized and marketed. As "face" belongs to personal biological information, with recognizable personality attributes, after technical processing and use, it will form data with commercial value, and it is very likely to generate the risk of being stolen "face" information. For example, AI face-swapping technology can realize "face exchange", but a series of legal problems have arisen in the process of storing and using face information. According to the classification of traditional sectoral laws, this paper will dig out the existing problems from civil and criminal aspects respectively.

2.1 Violations

2.1.1 Violating personal face information and threatening personal information security

"As the basic element for recognizing a person, the face plays an important role in daily life. The fusion of technology and the face has resulted in technology products that utilize information technology and incorporate the features of the face to bring convenience to people's lives, such as face recognition technology. At the same time, AI face-swapping technology, which was initially created for entertainment purposes, has been widely used in people's daily lives; AI face-swapping technology seems to achieve entertainment effects and satisfy people's curiosity about face-swapping, but in fact, it puts face information protection in a difficult situation. The protection of "face" information is in trouble.

The application takes advantage of the fact that customers do not pay much attention to the "notice and consent",

and sets up some contents in the terms and conditions that seriously infringe on the rights of users. Face information is not only personal information, but also an important part of sensitive personal information. Face information plays an important role in the protection of personal information. Face information is less private than other sensitive personal information such as "specific identity, financial accounts", and it is impossible and unnecessary to follow the protection measures for sensitive personal information such as "specific identity". According to the relevant laws in force in China, i.e. the Civil Code and the Personal Information Protection Law, the rules for handling sensitive personal information focus on the lawful handling of that information, while the legal regulation of the privacy of private information focuses on the passive defense against the unlawful disclosure of other people's privacy. In other words, it requires other citizens to refrain from certain behaviors that violate the right to privacy, while the rule on sensitive personal data is a positive obligation that requires the processors of said personal data to effectively fulfill the corresponding legal obligations [1]. In the process of using AI face-swapping technology, the processor of personal information, i.e., the applicant, should fulfill the corresponding legal obligations to guarantee the security of personal face information in strict accordance with the law.

2.1.2 Violation of the right to portrait and reputation.

The material library of AI face-swapping software provides users with a large number of "face-swapping" templates, and users can choose their favorite "faces" for synthesis. Through case studies and actual research, the author found that some software materials are obtained through illegal channels, and the faces of other people are used for profit-making activities without their consent.

A face contains the facial features of an individual, is recognizable, and is part of a portrait. The use of AI face-swapping technology that infringes on the portrait rights of others should be penalized by law. In addition, the malicious use of other people's face photos to generate images without the consent of the right holder negatively affects the right holder's reputation, and at the same time infringes the right holder's right to portrait and reputation.

2.1.3 Infringement of copyright.

Application developers providing users with material of unknown origin not only increases the risk of infringement of the right holder's portrait and reputation rights, but also raises the risk of infringement of the right holder's copyright. In a case concerning AI face-swapping software on the China Judgement and Documentation Network, it appeared that a certain AI face-swapping software illegally included pictures and videos taken by others in the software's material library. According to the relevant provisions of Articles 52 and 53 of the Copyright Law of the People's Republic of China, the copyright enjoyed by the right holder is infringed by the application developer, and the effective protection of the legitimate rights and interests of the copyright holder is an important element in the development and regulation of AI face-swapping technology.

2.2 Criminalization

2.2.1 Fraud.

In recent years, the trend of utilizing AI face-swapping technology to commit online fraud has intensified. How to effectively prevent and punish the use of AI face-swapping technology to commit fraud is an issue that should be focused on at present. The perpetrator, with the purpose of illegal possession, uses AI face-swapping technology to fictionalize the facts, and fraudulently obtains a large amount of public and private property, which is no longer limited to the traditional telecommunications network fraud, i.e., telephone and SMS methods. This type of fraud is more credible, leading to an increasing number of cases of telecommunications network fraud, which has greatly increased the rate of people being cheated in their daily lives.

2.2.2 The crime of manufacturing, trafficking and disseminating obscene materials.

In addition, the offenders utilized AI face-swapping software to generate obscene content for illegal dissemination. According to the relevant provisions of Section IX of the Criminal Law of the People's Republic of China, "The Crime of Making, Trafficking and Distributing Obscene Articles", the offenders shall be held criminally liable and sentenced to criminal punishment. Compared with the traditional crime of producing, trafficking and disseminating obscene materials, the use of AI face-swapping technology to commit such criminal acts accelerates the speed of dissemination, increases the harm, and is very likely to adversely affect the reputation of the right

holder.

To summarize, whether from the perspective of civil law or criminal law, it is not difficult to find that legal risks lurk in all aspects of the use of AI face-swapping technology. In order to propose practical solutions, the causes of the above legal problems caused by the use of AI face-swapping technology are worth exploring in depth.

3. ANATOMY OF THE REASONS FOR THE LEGAL PROBLEMS OF AI FACE-SWAP VIDEOS

3.1 Simulation and convenience of AI face-swapping technology

AI Face Swap utilizes deep compositing technology to synthesize new face images. Initially, it took a while to synthesize using this technology, but now the time has been reduced to a few dozen seconds, and the operation is extremely simple. Users only need to upload their own face images and select the material to realize the "face swap". This technology puts the public in an information scene where it is difficult to distinguish between reality and reality, breaking the social consensus that "face is real" and causing "distortion" on the cognitive level [2].

AI face swap technology no longer requires professional photographers and post-production staff to perform complex operations compared to traditional face swap technology, greatly reducing these requirements. Users only need to upload two face images to quickly generate a new face swap image. The emergence of this technology makes it easy for ordinary people to realize the face-swapping effect, greatly increasing the popularity of face-swapping technology. It is the simulation and convenience of this technology that provides an opportunity for perpetrators to illegally use AI face-swapping to commit illegal and criminal acts.

3.2 Interactivity and complexity of the network environment

AI face-swapping arises from the network and spreads in the network. As a form of production organization and medium of communication, the network can organize loose individuals [2], forming a dense Internet, which is conducive to the dissemination of network information. Due to the virtual nature of cyberspace and the anonymity of personal information, it is difficult to restrain the behavior of Internet users in network life, resulting in a series of legal problems. In addition, the network platform will produce a large amount of new information every day, interweaving into an intricate "network", which makes it more difficult to retrieve information, collect evidence and track suspects, resulting in more and more perpetrators using the network to commit crimes, which breaks through the traditional spatial limitations of criminal behavior.

3.3 Inadequate regulatory mechanisms for online platforms

At the beginning of the creation of Internet platforms, the concept of "agent-based regulation" was proposed and adopted, which means that enterprises should assume the responsibility of controlling the dissemination of information, and if they find illegal information on their business platforms, they should block, record and report the information to the relevant authorities in a timely manner, in order to solve the problem of regulating the dissemination of massive amounts of information. Compared with the principle of "enterprises are not responsible for the information published by others" established at the beginning of the development of the Internet in Europe and the United States, Chinese Internet enterprises have assumed more responsibility for assisting in the regulation of the Internet at the beginning of its development [3]. This kind of supervision idea has both advantages and disadvantages, on the one hand, enterprises themselves generate a lot of information and are more familiar with the technology and mechanism of network information, and can solve many problems of network information from a more professional perspective. However, in the actual supervision process, some enterprises do not seriously undertake the obligation to assist in the supervision, and even lower the regulatory bottom line for the sake of economic interests, which creates conditions for the actors to get out of the regulatory constraints. In addition, although the government's intervention has had a certain positive impact on the regulation of online platforms, there are still shortcomings. The government intervenes in the online market by means of public power to regulate and supervise from a macro perspective, which is more authoritative and mandatory. However, because the network market has been in the process of technological iteration and information generation, too much government intervention will, to a certain extent, limit the development of the network market, which is not conducive to stimulating the vitality of the network platform. China's current administrative supervision of personal information protection is characterized by weak objectives, scattered subjects, weak measures and vague procedures, which seriously impedes the improvement of personal information protection [4].

3.4 Ineffective judicial remedies

The potential legal risks of AI face-swapping technology, if not regulated and supervised, will become real legal problems. When rights holders find that their legitimate rights and interests have been infringed upon, it is difficult for them to find timely and effective judicial remedies. Application providers shirk their responsibilities by signing "informed consent" or choosing "silence", etc. Combined with the simulation and convenience of AI face-swapping technology itself, the interactivity and complexity of the network environment, etc., AI face-swapping technology can be used for a variety of purposes. Combined with the simulation and convenience of AI face-swapping technology and the interactivity and complexity of the online environment, the rights and interests of right holders in the online world cannot be effectively protected as in the real world.

3.5 Low legal awareness among users

In the process of using AI face-swapping technology, users are often driven by the curiosity of "face-swapping" and neglect the safety of personal face information. In addition, in the virtualized and anonymized cyberspace, the cyber world does not have the strict legal constraints of the real world, and some lawless elements take advantage of this to disseminate undesirable information, which many users pay close attention to and forward, but fewer users are able to soberly realize that this is helping lawless elements to spread and report to the relevant departments in a timely manner, but instead continue to spread, exacerbating the damage to the victims.

4. SOLUTIONS TO LEGAL PROBLEMS IN AI FACE SWAPPING

4.1 Sound tracking system for AI face-swapping applications and improved cybersecurity technology

Pictures and videos generated by AI face-swapping technology are highly simulated and hidden, making it difficult for network users to recognize the real from the fake. In order to solve this real problem and improve the security of AI face-swapping technology, the pictures and videos generated by AI face-swapping should be labeled as generated by AI face-swapping, reminding network users that this is not a real picture or video, so as to reduce the probability of network users suffering from fraud. At the same time, the establishment of a sound AI face-changing tracking system is one of the most important measures to prevent lawbreakers from using this technology to commit illegal and criminal acts. After users use AI face-swapping technology for network dissemination, the network system will be able to track the dissemination path of the generated content, providing convenience for law enforcement and judicial departments to investigate cases and collect evidence.

The technology itself is neutral, but its use has been restricted or prohibited due to the illegal intentions of some users; AI face-swapping technology is intended to provide users with a "face-swapping experience", but the developers of the technology did not anticipate that it would lead to so many legal issues when they developed the technology. Application developers should not prevent the use of the technology because of its drawbacks, but should choose the most appropriate technology to collect and store users' personal information according to the actual data security requirements of AI face-swapping, so as to effectively safeguard users' personal information and prevent the leakage of users' personal information. Coupled with the fact that the user's face information belongs to personal sensitive information, once leaked, it will provide raw data for lawbreakers to implement illegal and criminal behavior. Therefore, it is urgent for application developers to improve the security coefficient of AI face replacement technology.

4.2 Enhancing the "self-regulation" of online platforms and clarifying the responsibilities of online platforms

Online platforms not only enjoy the rights of organizers, but also need to play the role of self-regulation and increase internal oversight.

Although traditional criminal justice adheres to the principle of technological neutrality and applies the safe haven rule to infringements committed through online platforms, which are dealt with leniently, with the updating and development of judicial concepts, penalties for criminal acts of online infringement have become increasingly severe. On the criminal side, law enforcement has been strengthened through preparatory acts and common crimes; on the civil side, the scope of responsibility of online platforms has been expanding and penalties have been increasing. Through criminal and civil measures, the responsibility of online platforms has been recognized and resolved [5]. In the cause analysis, the problem of network platforms avoiding legal responsibility is also

mentioned, and the legitimate rights and interests of right holders cannot be effectively safeguarded. To implement the responsibility of network platform, we can start from the two aspects of improving the system of laws and regulations and clarifying the main body of network platform responsibility. First, the system of laws and regulations must be improved. The legislature should strengthen the legislative work of the network platform, formulate relevant laws and regulations, clarify the rights and obligations of the network platform, regulate the operation behavior of the network platform, and ensure the healthy and orderly development of the network platform. Secondly, it is necessary to clarify the main body of the responsibility of the network platform. The main body of network platform responsibility includes network platform operators, managers and participants. The operator is responsible for the daily operation and maintenance of the network platform of enterprises or individuals; the manager refers to the network platform for supervision and management of the department; the participants refer to the use of network platform users. The three are interconnected in the network platform and bear different responsibilities in different types of cases.

4.3 Improve the governance mechanism of the major regulators , and learn from the experience of "penetrating regulation" system

It is difficult to practically guarantee the effectiveness of supervision by only the network platform itself, and the role of network supervisory departments at all levels should be brought into play to strictly supervise and review network information. At present, China has formed a network regulatory mechanism coordinated by the Internet Information Office and coordinated by the Information Management Bureau, the public security authorities and the Market Supervision Bureau. In order to maintain a clean and positive online environment, the network regulatory mechanism should further clarify the specific division of labor and responsibilities, and draw on the experience of the "penetrating supervision" system to manage online platforms in a coordinated manner.

The first step in integrating the two organically is to clarify the responsibilities of network regulators at all levels. At the central level, the State Internet Information Office (SIIO) and the Ministry of Industry and Information Technology (MIIT) play a coordinating role, while at the local level, departments at all levels work together. Among them, the National Internet Information Office (NIIO), or "Net Information Office" for short, is also the coordinating and harmonizing authority for online personal information protection, and is mainly responsible for regulating the "content of Internet information". In addition, localities have specialized Internet Information Offices to actively protect local information security. In addition to the regulatory role played by the above departments, there is also the APP Specialized Governance Working Group set up jointly by major departments and associations, which is responsible for evaluating the privacy policies and the collection and use of personal information of application software with a large number of users and closely related to people's lives. Currently, the APP Special Governance Working Group has released a number of non-compliant APPs on online platforms, reminding users to use APPs with caution, which has greatly reduced the probability of infringement or crime cases. All regulatory authorities should strictly follow the relevant regulations and perform their respective duties to form an orderly and rigorous regulatory system.

The second step is to draw on the experience of the "through-and-through supervision" system. In exercising their supervisory powers, supervisory authorities at all levels can draw on the experience of the "through-and-through supervision" system in the financial sector. Conceptually, the platform penetrating supervision "penetrates" the innovative business model of the Internet and directly refers to its substantive function; in terms of means, the platform penetrating supervision "penetrates" the "legal veil" of the platform enterprises in order to avoid their own responsibility, and invasively carries out the supervision of the platform enterprises. From the means, the platform penetrating regulation "penetrates" the "legal veil" of the platform enterprise to avoid its own responsibility, and invasively carries out the process regulation, element regulation and algorithmic regulation [6]. When a new business model emerges on an online platform and causes problems, the existing regulatory framework does not have a corresponding focal point, and it is difficult to find the applicable legal basis, and at this time, the "penetrating regulation" system needs to play a role. Different from the traditional network supervision department, "penetrating supervision" emphasizes the directness and substantiality of supervision. While building a sound network supervision and management mechanism, drawing on the experience of "penetrating supervision" will be more conducive to maintaining personal information security and promoting the development of the digital economy.

From the above division of functions, it can be found that network regulators mainly supervise network platforms through administrative means. Although there is a full range of regulatory agencies, few of them are able to directly and effectively supervise enterprises. If we can learn from the experience of the "penetrating supervision"

system, and give the APP special governance working group more power to effectively supervise, it will help to strengthen the supervision, achieve better regulatory effect, and effectively restrain the online behavior of enterprises and online platforms.

4.4 Improving Blockchain technology to enhance the efficiency of judicial remedies

Blockchain technology, as a distributed database technology with features such as decentralization, data tampering, security and reliability, has been widely applied in recent years in the fields of finance, supply chain and Internet of Things. However, in the field of judicial relief, the application of Blockchain technology is still in the primary stage. To promote the application of Blockchain technology in the field of judicial remedies, Blockchain technology can be improved in the following aspects: first, establish a perfect legal and regulatory system, which is the basis for improving Blockchain technology. Clearly define the scope of application, authority and responsibility of Blockchain in the field of judicial relief. At the same time, it is necessary to protect the privacy and information security of citizens and prevent Blockchain technology from being abused. Secondly, the application of Blockchain technology in the field of judicial relief should be broadened, and the deep integration of Blockchain technology with the judicial system should be promoted. In addition, it is necessary to strengthen the application of Blockchain technology in the trial of cases, collection of evidence, and execution of judgments, so as to improve the efficiency of judicial remedies. Blockchain technology has a wide range of application fields, including electronic evidence, the ownership status of digital property and other fields. At the level of the trust mechanism, the encrypted data in the Blockchain cannot be tampered with and can be directly deposited. As Blockchain data is uploaded with timestamps, and these timestamps have consensus nodes to realize majority correctness, minority error correction, joint verification and recording, so the uploaded information can not be tampered with, and we can choose any time node to check the status, and we can choose any time period to check the authenticity of the data [7]. The application of Blockchain technology in the field of electronic evidence provides convenient conditions for solving the problem of collecting difficult evidence, and saves a lot of time and energy, and improves the efficiency of judicial relief.

Third, innovative application scenarios. Expanding the application scope of Blockchain technology in the field of judicial remedies is an important element in enhancing the efficiency of judicial remedies. New application scenarios of Blockchain technology in the field of judicial remedies, such as smart contracts, electronic evidence, online arbitration, etc., should be actively explored. The application of Blockchain technology in the field of judicial remedies requires continuous technical research and development and innovation. Investment in the research and development of Blockchain technology should be increased, and enterprises and research institutions should be encouraged to carry out technological innovation to improve the application of Blockchain technology in the field of judicial remedies.

Improving Blockchain technology and enhancing the efficiency of judicial remedies require the joint efforts of all parties, including government departments, judicial organs, enterprises and research institutions. By establishing a perfect system of laws and regulations, promoting the in-depth integration of Blockchain technology with the judicial system, innovating application scenarios and strengthening technological research and innovation, it is expected to promote the wide application of Blockchain technology in the field of judicial relief and inject new vitality into the development of China's judicial career.

4.5 Users to take timely and effective remedies to actively safeguard their legitimate rights and interests

In the Internet era, software or program development is endless, and it is difficult for regulators to strictly regulate them one by one. Therefore, in the process of regulation, the users themselves also play an important role. The network platform will produce a large amount of network information, software, programs, etc., every day, the user should pay attention to the legitimacy of each link in the process of use, and actively safeguard their legitimate rights and interests.

When utilizing AI face-swapping software, users are first required to sign an "Informed Consent Form" and be sure to read the contents carefully. The "Informed Consent" generally includes the "User Agreement" and the "Privacy Policy", which should be in line with the specific provisions on notification and consent in the handling of personal information as stipulated by the state. In order to better protect the rights and interests of users' personal information, the State Administration for Market Supervision and Administration and the State Standardization Administration issued GB/T 42574-2023 "Implementation Guidelines for Informing and Consenting in the Handling of Personal Information in Information Security Technology" (hereinafter referred to as the "Guidelines")

on May 23, 2023, which came into effect on December 1, 2023 onwards. The Guidelines stipulate in detail the applicable circumstances, basic principles, contents, methods and implementation of "notification and consent". When users find that the content of the "informed consent" violates the relevant provisions, they can raise objections to the software, and if the application provider fails to make modifications in accordance with the relevant content of the Guidelines, they can report the case to the relevant network regulatory authorities to safeguard the legitimate rights and interests of Internet users.

Users are consumers of Internet services and should enhance their awareness of self-discrimination in the face of emerging new technologies, programs and software. If they find any serious infringement of personal information security on the Internet platform, they should report it to the supervisory authorities in a timely manner, take effective measures to prevent the dissemination of personal information, prevent their own personal information as well as the personal information of others from being leaked or illegally used, and safeguard the rights and interests of personal information.

5. CONCLUSION

With the rapid development of technology, AI face-swapping technology has become an emerging visual processing technology. This technology utilizes deep learning and image processing algorithms to replace the facial features of one person with those of another, creating a "face swap" effect. While it brings some fun and convenience, it also poses a series of legal risks. The widespread use of this technology raises serious questions about the security of personal information, leading not only to civil infringements but also to criminal offenses. It is worth noting that the use of AI face-swapping technology is based on personal face information, which is personal sensitive information. Once personal sensitive information is leaked, it is very easy to jeopardize the personal and property safety of individuals. At the same time, personal information, as a basic source of data operating in the network era, is also an important protection object of the network rule of law.

Therefore, regulating the use of AI face-swapping technology is a matter of urgency. In view of the special characteristics of cross-border integration and cross-border development of network platforms, modern network regulation should strengthen the integration of regulatory means, establish and improve cross-sectoral and cross-regional "collaborative regulatory mechanism", create an all-round network platform regulatory system, and promote the formation of a synergistic situation of scientific and technological innovation, enterprise self-regulation, platform autonomy, public supervision and public participation. The system will promote the formation of a synergistic situation of technological innovation, enterprise self-regulation, platform autonomy, public supervision and public participation. Through the standardization of technology, collaborative supervision, clear responsibility, enhance legal awareness and other positive actions to regulate the use of AI face-swapping technology, to protect the personal information security of Internet users. The development and use of technology requires the "self-awareness" and responsibility of application developers, close supervision by regulatory agencies, and increased public awareness of the rule of law on the Internet. In order to build a network society based on the rule of law, technology, platforms, enterprises and the public should make concerted efforts to build a network security barrier and maintain a clean and positive network environment.

ACKNOWLEDGEMENTS

Funded by: This paper is the research result of the project of "Innovation and Entrepreneurship Training Program for College Students" of Sichuan Normal University in 2023--"Legal Problems and Solutions in AI Face Swapping under the Background of Network Rule of Law. --Based on the empirical research and analysis of the application of AI face-swapping" (Project No. x202310636273).

REFERENCES

[1] Wang Liming. Fundamental Issues in the Protection of Sensitive Personal Information--Background of the Interpretation of the Civil Code and the Personal Information Protection Act[J]. Contemporary Law,2022,36(01).
[2] Lin Aijun, Lin Qianmin.Technological Risks and Multiple Regulation of AI Face Swapping[J]. Future Communication,2023,30(01).
[3] Zheng Zhihang. Dualistic Co-Governance of Legal Governance and Technological Governance in Cybersociety[J]. China Law, 2018,(02).

[4] Wang Rong. Historical Development, Characteristics and Key Trends of China's Internet Regulation[J]. Information Security and Communication Secrecy,2017(01)
[5] Deng Hui. Legislative Options for Administrative Regulation of Personal Information Protection in China[J]. Jiao Tong University Law,2020(02).
[6] Shi, Wei. Legal Liability for Infringing Citizens' Personal Information through Online Platforms. China court website.2023-03-02.
[7] Zhang Linghan. Rationale and Limits of "Penetrating Supervision" of Platforms[J]. Legal Science (Journal of Northwestern University of Political Science and Law), 2022,40(01).
[8] Li Jialun. New thinking and application of Internet law [M]. Beijing:People's Publishing House,2022.2.