Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 2, No. 3, 2023

Legal Exploration of AI Face-Changing Technology

Huaiyuan Xu *

Department of Law, Dalian Ocean University, Dalian Liaoning, 116000, China
*** Corresponding author Email**: huaiyuanxu@126.com

Abstract: The present society is in a period of rapid development of artificial intelligence, and the process of its swift advancement is filled with both opportunities and challenges. As a branch of artificial intelligence, deep synthesis technology gradually enters people's vision. The significant technological innovations in the field of artificial intelligence have brought convenience to social life, but also conceal many risks. Emerging technologies pose significant challenges to personal rights, national security, social security, and judicial systems. Existing regulations have shown apparent lagging behind in response to emerging technologies. Relevant laws and regulations should be timely improved according to the trend of technological development, allowing emerging technologies to gradually operate within the framework of the rule of law while regulating their potential risks during the application of these technologies.

Keywords: Deep Synthesis; Artificial Intelligence; AI Face Changing; Personality Rights; Legal Regulation.

1. Overview of the AI Face-changing Technique

AI face-changing technology, actually known as deep synthesis technology, originated from "deepfake" technology, which is a new technology that uses electronic information data to simulate human faces and generate counterfeit audio-visual materials. Unlike earlier audio-visual simulation and counterfeit technologies, AI face-changing is more mature and intelligent, hence the name "AI face-changing." This technology has high application value in various fields, for example, it can present audio-visual materials more realistically in education, and produce more realistic and low-cost movie special effects in the film industry. Moreover, it can provide new directions for various media operations, such as virtual radio hosts, virtual idols, and virtual client service personnel. However, once this technology is abused, it may pose risks to national security, personal and corporate legitimate rights and interests. The underlying logic of this technology is to use and analyze biometric information. According to the General Data Protection Regulations, facial and iris information that has biometric attributes is highly sensitive information. In China's Personal Information Protection Law, biometric information that can identify facial features is considered sensitive personal information that may have a significant impact on important interests. Once this information is leaked, it may seriously jeopardize personal and corporate legitimate rights and interests and become a new tool for infringement and illegal activities.

2. The Application of AI Face-changing Technology

At the end of August 2019, an app named "ZAO" spread rapidly among the public with its AI face-swapping feature, which was essentially an application of shallow-depth deep synthesis technology. After registering, users only needed to upload a clear photo of their face, and they could enjoy a high-quality face-swapping service that combined their face with any video in a short amount of time. The facial fusion effect was excellent and could fully achieve a realistic result. Within less than a day, the app climbed to the third most downloaded app in major app stores and even made it to the top of Weibo's hot search list. However, the user agreement associated with "ZAO" caused widespread criticism. The agreement claimed that the uploaded images were "completely free, irrevocable, indefinitely transferable, and irrevocably licensed". The public's collective concern over privacy and security led to revisions of the user agreement and caused the software to be removed from the market for correction. The anxiety brought about by collecting and processing sensitive information from registered users caused every user of the software to become anxious.

Although the app provided special prompts at the beginning of the user agreement, it did not gain public trust. Besides the risk of compromising user privacy, the app also faced legal issues related to online payment risks, infringing on the right to personal image, and infringing on intellectual property rights. Because users inserted their faces into other videos without obtaining the authorization of the copyright owners, such action violated China's Copyright Law. Although the app did not directly participate in the production of infringing videos, it provided favorable conditions for such actions. Although the app did not charge users directly, it opened up many commercial projects and kept consuming traffic to earn a profit. Therefore, it was difficult to ensure that "ZAO" would not infringe upon others' rights.

Currently, there are multiple "face swapping" apps available, and previous facial recognition apps had their information maliciously tampered with. These apps have been used to conduct illegal activities such as taking advantage of scams, providing pornography services, and disseminating rumors.

3. The Existing Regulatory System and the New Rules Highlight

The existing legal regulations on AI face-changing technology mainly include the Civil Code, the Regulations on the Governance of Internet Ecology, the Regulations on the Administration of Internet Audiovisual Information Services, and the Regulations on the Administration of Internet Information Services for Deep Synthesis. However, due to the overly broad scope of the Civil Code and the first two

regulations, the National Internet Information Office released the Regulations on the Administration of Internet Information Services for Deep Synthesis on November 3, 2022, which will be implemented from January 10, 2023. This is China's first specialized departmental regulation governing "AI face-changing" or deep synthesis services, which regulates the management of face-changing technology, clarifies the objects of governance for generated synthetic algorithm, establishes the basic principles of algorithm governance, encourages relevant industry organizations to strengthen industry self-discipline, and establishes sound industry standards, guidelines, and self-regulatory management systems. It strengthens the main responsibilities of face-changing service providers and technical supporters and provides guidelines and norms for the application of technology.

The highlight of this regulation lies in the clarification of the responsibility of AI face-changing technology service providers, strengthening the implementation of access rules for users of AI face-changing technology, and requiring the service provider to store and manage the information analyzed by the AI face-changing service. This ensures that there is a management plan, traceable evidence, and a legal basis for accountability. For illegal activities using this technology, a negative identification list is established to quickly identify the illegal behavior of the user. A sound user management system is established with the formulation and public announcement of management rules to strengthen AI face-changing content management. If a perfect clarification mechanism, appeal channels, and reporting methods can be established, then the impact of rumors and false news caused by face-changing will be minimized.

This regulation imposes high requirements on AI face-changing service providers, requiring them to take responsibility for the platform and establish sound platform management mechanisms and technical security measures. The platform is required to ensure that every user knows and signs the platform convention and to demand that every service user provides their true identity information. If they fail to provide real identity information or if their identity information cannot be verified, they shall not be provided with services.

Regarding the implementation of responsibilities, the regulation indicates that AI face-changing providers and technical supporters who violate this regulation shall be punished in accordance with relevant laws and administrative regulations; for those who cause serious consequences, they shall be punished severely according to law. If it constitutes a violation of public order and administration, the public security organs shall impose administrative penalties in accordance with the law; if it constitutes a crime, criminal responsibility shall be investigated in accordance with the law. However, there is no specific definition of what constitutes "serious consequences" and how civil, administrative, and criminal liabilities are connected.

4. The Inadequacies of Current Legal Regulatory Methods

4.1. Civil Rights Protection is Costly and Administrative Responsibility is Difficult to Enforce

In terms of civil liability, AI face-swapping technology has a low threshold and cost, and its universality means that the perpetrators of illegal activities are often more concentrated on individuals rather than network platforms. Even if an audit mechanism and tracing database are established, in practice, they are mostly a kind of management after the fact. The internet world is vast and once uploaded to the internet, it is like scattered dandelions in the air, making it very difficult to protect one's rights. In terms of administrative responsibility, the specific exercise of power by the responsible parties involved in this technology's administrative and public security responsibilities, the scope of cases accepted by administrative agencies, and the specific administrative remedies available to victims are all unclear.

4.2. Criminal Law has Not Yet Included Deep Synthesis Technologies Such as AI Face-Swapping in Regulatory Frameworks

In terms of criminal responsibility, China's Criminal Law only includes the dissemination of false information related to military, danger, pornography, and other specific content. Most of the fake information dissemination problems involved in deep synthesis videos are civil tort issues. If the technology is not used for rumors, fraud, theft, etc., then most AI face-swapping videos currently available do not fall under the regulatory framework of criminal law. However, synthetic fake videos often have a strong social impact and become new opportunities and tools for criminal behavior. A significant limitation of legal regulation is that it is often a form of after-the-fact regulation. Due to the high degree of authenticity of AI face-swapping technology, according to current network platforms, rumors may be endlessly amplified. Even if there are strong legal regulations later on, the impact of the spread has already occurred. This is known as "rumors make people talk while refutes wear them out." Therefore, regulation of deep synthesis technology cannot simply stop at after-the-fact regulation, and mid-term and pre-regulation are extremely important.

4.3. Challenges to the Existing Judicial System.

In terms of the judiciary, AI face-swapping technology can create false videos and audio with very high credibility. If malicious actors use them, they will pose a significant challenge to the judicial system. The basic principle of all countries' justice systems is "based on facts and governed by law." Facts require evidence to support them. Audio and video materials are usually important evidence in litigation to support their respective claims. Judges must judge cases based on existing evidence and the opinions of all parties, and consider existing laws to make a guilty or not guilty verdict, and determine the severity of the punishment. If there are not enough technologies to differentiate deep forgery from real footage, or the difficulty of producing fake footage is too low, or the illegal cost of using deep synthesis is too low, and lacks legal regulation, then deep synthesis technology will have a huge impact on the existing legal system.

5. Recommendations for Legal Regulation of AI Face-changing Technology

5.1. Establish a Reasonable Regulatory System

Currently, there is no highly accurate technology for detecting fake videos in the field of artificial intelligence, and

network platforms do not have the ability to distinguish between user-generated videos and third-party uploaded videos that utilize deep synthesis technology. Therefore, the primary requirement for network platforms is to delete content promptly upon receiving complaints from copyright holders. It is not appropriate to ask platforms to judge and identify the content and sources. Moreover, it is essential to require creators and uploaders to label and disclose their deep synthesis works at the source of this technology. Each video maker should add clear identification markers after they produce each video. Any provider who offers services to remove, delete or alter these markers should be prohibited. This way, counterfeit products can be marked at the manufacturing stage, instead of leaving it up to market vendors and regulators to determine which is authentic.

5.2. Clarify the Legal Responsibility of AI Face-changing Product Makers

AI face-changing technology itself is neutral, and the ethical implications of using this technology depend on how it is utilized. Therefore, legislation should prohibit authoritative organizations, officials, and individuals from using this technology for creation and dissemination. Effective enforcement and punishment should be applied to those organizations and individuals who use AI face-changing technology to harm society and national security. Clear legal penalties must be established for individuals who attempt to commit crimes with this technology to deter them from doing so. Furthermore, a negative list of inappropriate AI face-changing use cases should be identified as soon as possible to restrict deep synthesis technology. Violators should be punished.

5.3. Gradually Strengthen the Legal Responsibility and Awareness of the Communication Media

Stopping the large-scale spread of AI face-changing-related false news during its dissemination is critical. Social media software is the most likely place for fake videos and audio to appear and spread quickly and widely. Social platforms are platforms where people with the same interests gather, so fake videos and audio are most likely to be uploaded and solidified. Therefore, it is crucial to clarify social software's legal responsibility on AI face-changing technology's false news harm to national security from a legal perspective. Through legal standards, social software's review mechanism and misinformation screening mechanism should be specified. We need to strengthen content review by prohibiting the uploading of false information that may endanger national security or cause negative social effects. The producers of AI face-changing videos that have no significant impact and are entertaining or beneficial to technological progress should be marked to inform the public of their falsity to prevent unnecessary social consequences. The social media platforms that do not meet their regulatory obligations and video makers who do not meet their labeling obligations must be held liable, and effective enforcement must be carried out.

5.4. Establish a Necessary Crisis Response Mechanism

When fake news is discovered, we must respond quickly, prevent the spread of false information and adverse effects from expanding. To accomplish this, administrative departments should strengthen exchanges and cooperation with social media, news agencies, non-governmental organizations, and other institutions, share AI face-changing related information channels, and ensure timely and effective disposal when significant false information is detected. Strengthen network supervision, improve the reporting system, delegate regulatory authority, expand regulatory subjects, and establish and improve the feedback and review system for reporting information to take action promptly when false information and videos first appear. Increasing the responsiveness of network supervisors, increasing the penalties for false information disseminators, and raising the reward standards for regulators and whistleblowers are powerful safeguards to enhance crisis response capabilities. Additionally, establishing and improving the crisis response department is an essential way to improve the ability to cope with false information crises caused by AI face-changing.

5.5. Strengthen Anti-counterfeiting Tracing Technology and Educational Propaganda Efforts

As AI face-changing technology continues to develop, corresponding anti-counterfeiting and tracing technologies should synchronize with its advancement to accurately identify and trace the source of messages and its origins resulting from AI face-changing technology. However, current academic and commercial anti-counterfeiting development projects are aimed mainly at specific products rather than universal audio and video content. In other words, it is necessary to construct and train a corresponding anti-counterfeiting network for each new type of emerging video content tampering technology, which lacks a general-purpose video anti-counterfeiting network. The developer of PhotoDNA technology said, "We are decades away from being able to identify AI face-changing content confidently." This means that we need to develop efficient and universal anti-counterfeiting technology urgently. Moreover, it is necessary to enhance educational propaganda throughout society to increase citizens' awareness and identification of deep counterfeiting and improve their identification skills. Users of social media must recognize the hazards of abusing AI face-changing technology, gradually improving their identification and prevention awareness, and treating AI face-changing audio and video materials critically by conducting multiple searches and verifications to prevent risks to promote the development and appropriate use of adversarial and identifying technology in the future.

6. Conclusion

AI face-changing technology has many positive implications for various aspects such as the economy, education, and culture. However, due to the lag of existing regulatory systems in regulating emerging technologies, it poses potential risks to personal rights and interests such as reputation, portrait, and identity; it also poses significant threats to national security, social security, and defense technology. In addition, the application of AI face-changing technology brings challenges to the existing legal system. "Technology has no ethics, but people who use technology have ethics." The AI face-changing technology itself is neutral, and only correct utilization can benefit humanity. The American experience provides us with sufficient enlightenment, while China's application of AI face-changing

technology is still in its infancy, and its risks have already been revealed. Therefore, we need to establish effective regulatory systems, including legislation and supervision, to effectively regulate AI face-changing technology and promote its positive effects while eliminating its existing risks through the rule of law.

Acknowledgments

This article was originally drafted in early 2020, when the COVID-19 pandemic broke out, causing all of my graduation plans to fall apart. I had planned to take some time to travel and say goodbye to my teachers and classmates in the second semester of my senior year, but instead everything was left with regret. That year, I took the postgraduate entrance exam for the first time and missed the cut off by one point. I felt helpless and heartbroken, but still had to move forward. Despite the dual pressures of failure and the pandemic, I completed the initial draft of this paper, which ultimately helped me successfully graduate from college and win an award for outstanding thesis.

In the years since my graduation, I have passed the postgraduate entrance exam and the national judicial exam. During this time, many of the systems mentioned in this paper have undergone significant changes, just as my life has undergone tremendous changes. However, the topic of this paper - the update and iteration of deepfake technology - has continued to be widely discussed. The backwardness of many systems has become increasingly evident, and the novelty of the topic remains strong. On this basis, I have revised this paper by integrating and summarizing the new legal rules released in recent years, comparing the problems discovered in 2020 with present realities, and comparing previous recommendations with the latest legislation. I found that many of the problems I previously pointed out have been resolved, and many of my suggestions have been adopted in new laws and regulations. For example, my suggestion to establish a system for identifying video sources and improving traceability mechanisms, both of which were proposed in 2020, have been adopted in new regulations. This has given me a sense of accomplishment and fulfillment.

I would like to thank my mentor, Dean Pei Zhaobin, for his strong support of this paper and his love and guidance over the past two years. I will always remember this as a student. This paper was also based on my undergraduate thesis, so I would like to thank my thesis advisor, Duan Ying, for her guidance. In addition, I would like to thank my roommate, Xu Chao, who is a computer engineering graduate student, for answering many questions in his area of expertise and for accompanying me through the ups and downs of this journey.

This road has been bumpy and challenging, but I am grateful that I did not let myself down.

References

[1] Zhang L.H. (2023). "Logical update and system iteration of deep synthesis governance: the Chinese path of generative artificial intelligence governance such as ChatGPT" (Journal article). Law Science (Journal of Northwestern University of Political Science and Law), 2023(03), 38-51. [2023-04-19].

[2] Lin A.J., & Lin Q.M. (2023). "Technical risks and multiple regulations of AI face-swapping technology" (Journal article). Future Communication, 30(01), 60-69.

[3] Yi R. (2023). "Real games: deep synthesis or deep forgery?" (Journal article). Secrecy Work, 2023(02), 48-49.

[4] Multi-scenario content production applications based on deep synthesis technology (Journal article). Broadcasting and Television Information, 2023, 30(02), 20-21.

[5] "Regulations on deep synthesis management of internet information service" (Journal article). Gazette of the State Council of the People's Republic of China, 2023(04), 22-25.

[6] Chang X.P., & Du Y.N. (2023). "Deep influence on media institutions and media industry development" (Newspaper article). China Press and Publishing Journal, 2023-01-17(008).

[7] "Three departments jointly issued new rules on deep synthesis, 'AI face-swapping' is restrained" (Journal article). Police Technology, 2023(01), 93.

[8] Sun W.C., Tian Q., Luo M., & Liu J. (2023). "Video deep forgery detection technology and application" (Journal article). Police Technology, 2023(01), 10-16.

[9] Zhang C., & Chen S. (2022). "Exogenous risk of deep synthesis and platform governance principles" (Journal article). Chinese Journalism and Communication Research, 2022(05), 39-49.

[10] Zhang W.X. (2003). "Marxist Jurisprudence: Theory, Method, and Frontier" (Book). Beijing: Higher Education Press.