Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/55/20240083

The Current Situation and Prevention of AI Telecom Fraud: Starting from Personal Information Protection

Lezhi Li[1,a,*]

[1]*School of Law, Guangzhou University, Guangzhou, China*
a. 32102100038@e.gzhu.edu.cn
**corresponding author*

Abstract: AI telecom fraud is an act of using artificial intelligence deep cooperation and analysis technology to create false information to lure and deceive individuals and illegal possession of money. With the rapid development of the Internet and AI, the number of AI telecom fraud cases has exploded, so how to prevent AI telecom fraud has become an important issue in society. AI telecom fraud has led to a series of problems, such as the illegal collection and malicious disclosure of personal information, criminals using AI to analyze personal information for fraud, and the industry does not adequately supervise the collection and use of personal information by companies. This article uses case analysis, normative analysis, and comparative research methods to analyze the above three problems and proposes the solution, including establishing a complete legal regulatory system for personal information protection and the prevention and control of AI telecom fraud, and strengthening industry supervision. It is hoped that by applying the above-mentioned solutions, the protection of personal information and the prevention and control of AI telecom fraud can be strengthened, and the development of AI telecom fraud prevention and control in China can be promoted.

Keywords: Artificial intelligence, Telecom fraud, Personal information, Prevention

1. Introduction

In recent years, AI technology has developed rapidly, bringing great convenience to human social life. However, as the technology continues to mature, the number of cases involving crimes using AI has also increased at a rapid pace. The development of AI technology in deepfake provides criminals with new technical support in the field of telecom fraud. Criminals use these technologies to commit telecom fraud, making the scam look more real, thereby inducing victims to transfer money to criminals. This type of fraud using AI technology has a high success rate, involves large amounts of money, and is extremely harmful to society. The high concealment, high realism, and high automation of AI telecom fraud make it more deceptive, more difficult to identify, and more harmful. The main reason for the rapid development of AI telecommunications fraud is the serious leakage of personal information. The 53rd Statistical Report on the Development of China's Internet, released by the China Internet Network Information Center (CNNIC), revealed that by December 2023, China's internet user count had risen to 1.092 billion, marking a rise of 24.8 million from the previous year, with an internet penetration rate of 77.5% [1]. Facial, fingerprint, palm print and voice recognition, which have become increasingly common in recent years, all involve citizens' biometric information.

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/55/20240083

If service providers do not manage the personal information properly or leak it maliciously, causing large-scale leakage of relevant information, it may be used by criminals in telecom fraud, seriously affecting social security. The correlation between personal information leakage and the advancement of AI telecom fraud is apparent. Safeguarding personal information undoubtedly stands as a fundamental strategy in addressing AI telecom fraud at its core. Specifically, it is to analyze from the perspective of the relationship between personal information leakage, personal information protection and AI telecom fraud, and draw conclusions about the prevention dilemma and prevention measures of AI telecom fraud.

2. The Impact of Telecom Fraud on Personal Information within the Framework of Artificial Intelligence

2.1. Overview of AI Telecom Fraud

2.1.1. Concept of AI Telecom Fraud

AI telecom fraud refers to criminals who use emerging technologies such as big data and AI, such as AI deep fake technology and AI program analysis technology, to achieve "AI face-swap" and "AI simulated sound " for the purpose of illegal possession, and chat with victims through phone, video, voice chat and online chat, use familiar faces, information or voices to gain their trust, carry out remote, contactless fraud, and induce victims to transfer money to them.

2.1.2. Characteristics of AI Telecom Fraud

AI telecom fraud is telecom fraud implemented using AI technology. This type of telecom fraud has the following characteristics.

First, the fraud methods are concealed and diverse. Criminals often use remote and contactless methods to commit fraud, using videos, phone calls, text messages, social application and other medium to commit fraud, using AI to deepfake faces and voices, creating false images, audio and video, and impersonating other people to commit fraud. There are currently 7 major types of telecom fraud and more than 60 methods. Second, fraudulent activities are organized and group-based. Most frauds are committed by gangs, who rent servers overseas and use fraudulent network platforms provided by operators on the Internet. The criminal gangs have clear division of labor, including technical personnel, fraudsters, and those who withdraw and transfer stolen money, showing the characteristics of organization and group-based. Third, the fraud methods are technological, difficult to identify and have a high success rate. AI telecom fraud uses AI deepfake technology to combine citizens' facial, facial expressions, voice and movements information with other people's videos and pictures. The forged videos, images and sounds are highly simulated and difficult to identify. Therefore, the success rate of AI crimes is higher than other telecom frauds. Fourth, it is difficult to combat fraud and recover the stolen money. Most fraud gangs often commit crimes without contact abroad, making it difficult to arrest them. Most fraud evidence is online information data, which is difficult to collect. Criminals often transfer the stolen money within minutes of the successful fraud, making it difficult for victims to take immediate action.

2.2. Analysis of the Current Status of Citizens' Personal Information Security under the Background of Artificial Intelligence

2.2.1. The Meaning of Personal Information

On May 9, 2017, the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information was issued by the Supreme People's

DOI: 10.54254/2753-7048/55/20240083

Court and the Supreme People's Procuratorate of China. It defines "citizens' personal information," as stipulated in Article 253 of the Criminal Law, as various information recorded electronically or otherwise, which can identify a specific natural person alone or in combination with other information, or reflect the activities of a specific natural person, including name, ID number, communication contact information, address, account password, property status, whereabouts, etc. The definition of personal information in this interpretation adopts a formal broad identifiability plus activity status elements, which is an interpretation that includes both substantive personal identity information and personal information that may pose a threat to personal life or property [2].

2.2.2. The Necessity of Protecting Personal Information within the Framework of Artificial Intelligence

In the era of big data, citizens' personal information is being used more and more frequently. Citizens' personal biometric information such as faces and fingerprints, is being used in life and is closely related to citizens' lives. However, as citizens' personal biometric information is used widely, the possibility of citizens' personal information being leaked and illegally used has greatly increased. For example, in May and June 2018, the defendants Deng and Lin purchased mobile phone cards and other tools, and gathered together the defendants Chen, Zhang and others, and used the purchased personal privacy information of citizens including telephone numbers, addresses, names, etc. to commit fraud, defrauding a total of 392,000 yuan. Between November 2015 and August 2016, Chen, Huang, Zheng, and additional defendants acquired personal information of students and citizens' housing purchase details through online platforms. Under the guise of providing scholarships and housing subsidies to financially disadvantaged students, they defrauded the candidate for college entrance examination, defrauding more than 560,000 yuan. It can be seen that citizens' personal information is an important tool for criminals to commit online fraud, and the importance of protecting citizens' personal privacy information is self-evident.

2.2.3. Threats to Personal Information under the Background of Artificial Intelligence

2.2.3.1. Illegal Collection of Citizens' Personal Information

Criminals use network attacks, such as virus attacks, data crawling, ransomware, etc., to use hackers' illegal links, QR codes and mobile phone apps to obtain citizens' personal information. Or they attack the servers of third-party service platforms through the network to illegally collect a large amount of citizens' personal privacy information and conduct AI telecom fraud.

2.2.3.2. Malicious Disclosure of Citizens' Personal Information

In the era of big data, third-party service providers require users to provide their personal information, such as facial information, ID card information, name, address, etc. when registering an account on the grounds of providing services. A large amount of citizens' personal information will be stored in the database of the third-party service provider. In addition, when citizens use software provided by third-party service providers, they may also leave personal voice messages, browsing histories, purchase records, IP addresses and other information. Even if the information collection method is legal and compliant, third-party service providers as recipients of personal information may abuse, share or sell citizens' personal information to loan companies or fraud gangs. In this case, it is difficult for citizens to find out that their information is being used illegally at the first time. This malicious disclosure of citizens' personal information is hidden and difficult to prevent.

DOI: 10.54254/2753-7048/55/20240083

2.2.3.3. Illegal Use of Citizens' Personal Information

After illegally collecting citizens' personal information, criminals use AI technology to create fake faces and voices with stolen facial and voice information to defraud the relatives and friends of the citizen, or use the citizen's personal information to borrow money from online loan companies. In addition, criminals also use stolen personal information to analyze the characteristics of specific citizens and carry out targeted fraud against them.

2.3. The Relationship between AI Telecom Fraud and Personal Information Leakage

2.3.1. AI Telecom Fraud Usage Scenarios

At present, AI telecom fraud can be divided into two categories: "AI face-swap, AI simulated voice" and "AI targeted fraud". The first category is that criminals collect citizens' facial and voice information, use AI to deeply forge the faces and voices of people familiar to the victims, and use video calls and phone calls to make the victims relax their vigilance against the criminals, thereby committing fraud. The second category is that criminals use AI technology to accurately screen and analyze citizens' personal information, and then use AI to generate customized fraud scripts to carry out targeted fraud, such as false investment recommendations, using false investment information generated by AI to induce users to invest in false projects and defraud funds.

2.3.2. AI Telecom Fraud Relies on Personal Information

Infringement of citizens' personal information is often the main upstream crime of telecom fraud. The illegal collection, malicious disclosure and illegal use of citizens' personal information will increase the success rate of AI telecom fraud. First, "AI face-swap" scams are mostly committed by criminals who use facial recognition models and cameras to obtain citizens' facial feature points, which are then used to forge a fake video. Collecting feature points will make AI face-swap forged videos more realistic. Criminals will collect a large number of images and videos of the victim's relatives and friends as AI face-swap materials before committing the crime. Second, the "AI simulated voice" type of fraud is that criminals obtain the voice information left by citizens on different platforms, analyze and imitate it through AI models, ultimately producing cloned human voices that are extremely similar to real people. Third, AI targeted fraud is that criminals use AI technology to accurately analyze citizens' personal information and carry out targeted emotional fraud or financial fraud, such as pig-butchering scam and false investment fraud.

3. Dilemma in Preventing AI Telecom Fraud Crimes in the Case of Personal Information Leakage

3.1. Imperfect Legal System and Mechanism for Personal Information Protection

3.1.1. Serious Personal Information Leakage

There are three types of citizen personal information leakage: negligent leakage, malicious leakage, and technical intrusion. Negligent leakage refers to the leakage of citizen personal information caused unintentionally by operators and service providers when they collect, use and store citizen personal information without adequate protection measures and lack information security awareness. Malicious leakage refers to the malicious sale of citizen information by operators and service providers in order to obtain huge profits. Both methods will cause serious leakage of citizen personal information [3]. Hacker network attacks are also a way for citizens' personal information leakage. Hackers will invade websites or personal terminals through technical means such as implanting

DOI: 10.54254/2753-7048/55/20240083

viruses and decoding attacks to gain control and obtain personal information from operators and service providers' databases or personal terminals.

Modern technology presents a lot of personal information in digital form, and digital personal information is transmitted through the Internet. The instantaneous nature of the Internet determines that personal information stored on the Internet will be transmitted in a more convenient way and at a higher speed. The world is connected by the Internet, serving as a conduit for global information dissemination. When personal information is leaked, it rapidly spreads across a broader spectrum through internet, posing a significant threat to personal information protection.

3.1.2. Incomplete Definition of Personal Information

Although the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information defines "citizens' personal information" in Article 253 of the Criminal Law, it is not perfect. Currently known AI telecom frauds mostly use citizens' faces, voices, IP addresses, or consumption information to commit online fraud. However, in the interpretation, due to the lag of the law, this information has not yet been defined as citizens' personal information. In addition, some judicial interpretations exclude personal biometric information from personal information, which is not conducive to the protection of personal information. This exclusion has a significant impact on determining whether fraudulent behavior in AI telecom fraud is suspected of infringing on citizens' personal information.

3.1.3. Imperfect Behavior Patterns in Crimes of Violating Citizens' Personal Information

Article 253 of the Criminal Law only defines the acts of selling, providing, stealing or illegally obtaining citizens' personal information by other means, and does not make explicit provisions for the negligent disclosure of citizens' personal information. Currently, there are many operators and service providers who negligently disclose citizens' personal information, and the Criminal Law is unclear about the negligent disclosure of citizens' personal information, which will make it difficulty in investigating the infringement of citizens' personal information by negligent disclosure.

3.2. Imperfections in Legal System and Mechanism for AI Telecom Fraud

3.2.1. Weak Punitive Measures for AI Telecom Fraud

AI telecom fraud is a downstream crime that infringes on citizens' personal information. A lot of citizens' personal information is used to carry out precision AI telecom fraud. However, currently AI telecom fraud is only punished according to Article 266 of the Criminal Law, which is not strong enough [4]. Especially in the context of artificial intelligence, AI telecom fraudsters can obtain more personal information of citizens, the methods of fraud are more covert, the amount involved is larger, the evidence of fraud is difficult to fix, and even overseas fraud gangs are involved. It is not enough to punish AI telecom network fraud with the crime of fraud alone, and the criminal behavior and punishment are not corresponding.

3.2.2. Lack of Relevant Legal Regulations on AI Crimes

Current laws and regulations lack content to regulate AI crimes, and there are no specific provisions on AI online fraud. This may result in AI crimes being unable to be regulated using current legal norms. At present, only some guiding opinions or management regulations mention AI crimes. For example, Article 8, Paragraph 4 of the Guiding Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on the Legal Punishment of Cyber Violence Crimes shows that those who use generative artificial intelligence technologies such as

DOI: 10.54254/2753-7048/55/20240083

"deep synthesis" to publish illegal information shall be punished more severely. This is only a regulation on AI publishing illegal information, and there is a lack of regulations on AI using citizens' personal information to commit online fraud.

3.3. Inadequate Supervision and Management of Personal Information in the Industry

The industry lacks relevant regulations on operators and service providers using AI to collect and use citizens' personal information. In particular, there is a lack of relevant regulations on the protection of citizens' faces, voices, consumption records, browsing records, and other personal information that can be easily used for AI telecom fraud. There is also a lack of relevant regulations on operators and service providers maliciously selling citizens' personal information to obtain huge profits.

3.4. Lack of Multi-party Cooperation Mechanism

A scholar believes that cooperation among service providers, governments, and users can greatly improve the ability to defend against online fraud and enhance the ability to identify cyber criminals. However, due to privacy issues, there is still a lack of a tripartite cooperation mechanism in the world, and a lack of a privacy protection mechanism for information providers, making it difficult to achieve tripartite protection collaboration [5].

4. AI Telecom Fraud Crime Prevention Measures from the Perspective of Personal Information Protection

4.1. Foreign Legal Regulatory Systems for Personal Information Protection and the Use of Artificial Intelligence Technology

4.1.1. US CCPA

The California Consumer Privacy Act (CCPA) is the first comprehensive privacy law in the United States. CCPA defines personal information as data that can directly or indirectly link to, describe, or reasonably associate with an individual or household. In addition, CCPA enumerates various data categories classified as personal information, such as name, IP address, mailing address, biometric information, Internet browsing or search history, geographic location, and any deductions made from these data types. The definition of personal information under CCPA is broad, including nearly all data linked to an individual.

4.1.2. EU GDPR and Artificial Intelligence Act

The EU's General Data Protection Regulation (GDPR) regulates the protection of personal information from the perspective of personal privacy rights, regulates personal information collectors and providers, and innovates in many aspects. First, GDPR stipulates that companies that handle personal information must review the companies that provide personal information and enter into contracts on data usage, data retention, etc., in order to limit the use of personal information. Secondly, the designers of GDPR believe that in data activities, most users are in a state of low voluntary consent to the terms, which is disadvantageous to users. Users will agree to the company's collection and use of their personal information in order to use the software, but GDPR makes low voluntary consent not a way to protect the legal use of personal data [6].

The GDPR expands the scope of personal data, including any information relating to an identifiable natural person. This includes evident personal particulars like a person's name and address, alongside any data capable of identifying an individual, such as their IP address and specific cookie identifiers linked to a web browsing session. On March 13, 2024, the European Parliament passed the

DOI: 10.54254/2753-7048/55/20240083

“world's first Artificial Intelligence Act", and on May 21, the European Council approved the bill. This bill will have a huge impact on the legal use of artificial intelligence technology in China and even the world. The bill regulates AI that threatens citizens' rights and prohibits systems that obtain citizens' facial information and other information in an indiscriminate manner, which can largely protect citizens' facial information. In addition, the bill stipulates the transparency of artificial intelligence system models, and users of AI technology need to mark images, videos, audio and other content processed by artificial intelligence.

4.2. Establishing a Sound Legal Regulatory System for Personal Information Protection

At present, Paragraph 1 of Article 253 of the Criminal Law of the People's Republic of China and Article 10 of the Personal Information Protection Law of the People's Republic of China have relevant provisions on the disclosure and use of personal information. However, with the rapid development of artificial intelligence technology, the definition of citizens' personal information still needs to be improved, and the state's protection of the right to control personal information has become particularly important.

4.2.1. Improvement of the Definition of Citizens’ Personal Information

Since AI telecom fraud is a downstream crime that infringes on individuals’ personal information, the implementation of the crime is highly dependent on individuals’ personal information. The personal information used by AI network fraud is relatively new information such as facial information, voice information, consumption information, browsing history, IP addresses, etc. Various data recorded electronically or otherwise can identify the identity of a specific natural person or reflect the activities of a specific natural person alone or in combination with other information. Consequently, such data should be regarded as personal information. However, there are currently no relevant laws and regulations that clearly define this information as citizens' personal information. Defining this information as citizens’ personal information and improving the definition of citizens’ personal information will help prevent and control AI telecom fraud. In view of this, we can refer to the definitions of personal information in the CCPA of the United States and the GDPR of the European Union, and include IP addresses, mailing addresses, biometric information, Internet browsing history or search history, geographic location, etc. into personal information, thereby expanding the types of personal information.

4.2.2. Improving the Protection of Personal Information Control Rights

The right to control personal information mainly refers to the right of citizens to control and make independent decisions on personal information, including the right of individuals to know when their information is collected and used, as well as the right of individuals to use the information and authorize others to use the information. Others’ right to control personal information is primarily infringed upon by the collection and usage of personal information without consent [7]. In the era of big data, citizens' personal information is mostly digitized and stored in databases on the Internet. The protection of citizens' right to control personal information becomes particularly important. Specifically, it is to protect citizens' personal information from being illegally collected and maliciously disclosed. The right to control personal information is essentially still a personal right and should be protected by laws and regulations.

DOI: 10.54254/2753-7048/55/20240083

4.3. Establishing a Sound Legal Regulatory System for the Prevention and Control of AI Telecom Fraud

Regarding AI telecom fraud, Article 266 and Paragraph 1 of Article 287 of the Criminal Law, and Article 46 of the Cybersecurity Law of the People's Republic of China have provisions on telecom fraud, Article 6 of the Regulations on the Management of Deep Synthesis of Internet Information Services, Article 4 of the Interim Measures for the Management of Generative Artificial Intelligence Services, and Article 8 of the Guiding Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on the Legal Punishment of Cyber Violence and Crime also have certain provisions on generative artificial intelligence network crimes, but there is still a lack of specific provisions on AI telecom fraud.

4.3.1. Adding the Crime of "Telecom Fraud" Related to Artificial Intelligence

One scholar believes that the crime of "telecom fraud" should be added to the Criminal Law, and that multiple related crimes should be included in this crime in order to better punish telecom fraud crimes [8]. AI telecom fraud is more covert, more deceptive, has a higher success rate, involves larger amounts of money, and is more closely related to citizens' personal information. It should be regulated as a "telecom fraud crime". In current judicial practice, judicial organs only treat telecom fraud crimes as ordinary fraud crimes, resulting in fraud gangs only having to pay a low behavioral cost but receiving high returns, and failing to make the criminal behavior and punishment commensurate. Therefore, the "telecom fraud crime" should be added, and AI telecom fraud should be regulated in it, so that criminals receive punishments commensurate with the criminal behavior they have committed.

4.3.2. Regulating the Use of Artificial Intelligence to Analyze Citizens' Personal Information

The currently released Interim Measures for the Management of Generative Artificial Intelligence Services and Regulations on the Management of Internet Information Service Deep Synthesis have made certain regulations on AI deep synthesis technology, but they only regulate AI activities such as using deep synthesis services to produce, copy, publish, and disseminate information prohibited by laws and administrative regulations. There is still a lack of regulations on the use of AI to obtain and analyze citizens' personal information. Laws and regulations should be used to regulate AI activities that may be used for criminal activities, such as using AI to analyze citizens' consumption records, browsing records, work information and other personal information in order to carry out targeted fraud and to generate targeted fraud scripts. Regulating the use of AI to collect and analyze personal privacy information will help prevent and control AI telecom fraud form the source, thereby reducing the number of victims.

4.4. Strengthening Industry Supervision

Since AI telecom fraud is highly dependent on personal information, when regulating and governing network fraud, it is necessary to strengthen industry supervision and management of operators and service providers' collection and processing of personal information. At present, some relevant documents are about to be issued. For example, in 2021, the Ministry of Industry and Information Technology, together with the Ministry of Public Security and other departments, drafted the Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications (Draft for Comments), which regulates the processing of personal information of mobile Internet applications by APP developers and operators. At present, some relevant documents are about to be issued. For example, in 2021, the Ministry of Industry and Information Technology, the

DOI: 10.54254/2753-7048/55/20240083

Ministry of Public Security and other departments drafted the "Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications (Draft for Comments)", which regulates the personal information processing activities of mobile Internet applications by operators who develop APPs. However, the draft for comments does not include any regulations on the use of personal information by developers and operators in AI deep synthesis technology. In the future, industry supervision should be strengthened on the use of citizens' personal information by developers and service providers using AI. The industry should supervise and manage the behavior of developers and service providers using AI to obtain, collect, and use personal information, establish industry rules and regulations and industry red lines, and punish developers and service providers who cross the red lines.

4.5. Tripartite Collaboration for Privacy Protection

The cooperation among service providers, the government and users in protecting personal privacy information can be strengthened. The government can regulate the collection, use and protection of personal information by service providers through rules and regulations, clarify the responsibilities and obligations of service providers when handling personal information, and strengthen supervision of service providers. Service providers should disclose to users the methods of information collection and use. An information sharing mechanism can be established among the three parties to ensure the legal use of personal information.

5. Conclusion

The rapid development of AI technology has provided new means and channels for telecom fraud, making the ways and means for criminals to obtain citizens' personal information and use citizens' personal information to commit telecom more covert and intelligent. A serious threat to personal information security and social stability is posed by the emergence of AI telecom fraud as a global criminal activity. Building upon this foundation, enhancing pertinent laws and regulations concerning personal information protection and AI telecom fraud, bolstering industry oversight of artificial intelligence technology, and fostering tripartite collaboration emerge as pivotal measures in combating AI telecom fraud. Through the study of the relationship between AI telecom fraud and the leakage of citizens' personal information, we hope to help improve the relevant laws and regulations on AI telecom fraud and personal information protection, and provide relevant ideas and solutions for judicial practice to govern AI telecom fraud.

References

[1] *China Internet Network Information Center. (2024). The 53rd Statistical Reports on Internet Development in China. Retrieved from https://www.cnnic.net.cn/n4/2024/0322/c88-10964.html.*

[2] *Yu Zhigang. (2017). The Right Attribute of "Citizen's Personal Information" and the Thought of the Criminal Law Protection. Zhejiang Social Sciences, 10, 4-14+155.*

[3] *Xiao Chengjun, Xu Yuzhen. (2017). Personal Information Leakage and its Multi-center Governance in big Data Era. Inner Mongolia Social Sciences, 38(02), 185-192.*

[4] *Zhao Lianqing. (2017). Criminal Law Protection of Citizens' Personal Information Security -- from the Perspective of Frequent Telecom Network Fraud Cases. Study & Exploration,09,80-84.*

[5] *Ali M A, Azad M A, Parreno-Centeno M, Hao F, van Moorsel A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. Future Gener. Comp. Sy., 100,408-427.*

[6] *Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius. (2019). The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98.*

[7] *Wang Liming. (2013). Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy. Modern Law Science, 35(04),62-72.*

[8] *Wang Xiaoxue. (2023). Research on the Prevention and Control of Telecom Network Fraud Crime: From the Perspective of Personal Information Protection. East China University of Political Science and Law.*