Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 7, No. 3, 2024
www.scholink.org/ojs/index.php/elp

Original Paper

Research on the Criminal Law Response to Telecom Fraud in the Digital Society

Yanqiu Xiong[1*] & Minna Qiu[2]

[1] The discipline inspection and supervision group of the Anqing City Discipline Inspection Commission in the Anqing Municipal People's Congress, Anqing, China

[2] Law School, Shantou University, Guangzhou, China

Received: October 10, 2024 Accepted: October 18, 2024 Online Published: October 19, 2024

doi:10.22158/elp.v7n3p33 URL: http://dx.doi.org/10.22158/elp.v7n3p33

Abstract

With the rapid development of the digital society, telecom fraud has increasingly exhibited characteristics of intelligence, cross-border operations, and concealment, posing serious threats to both the economy and individual interests. However, the current criminal law has many deficiencies in addressing such crimes, making it difficult to effectively curb their spread. This paper analyzes the current state and characteristics of telecom fraud and explores the shortcomings of criminal law in responding to these new forms of fraud in the digital society. It proposes measures such as enhancing the adaptability of the law, improving sentencing standards, and strengthening cross-border judicial cooperation. Furthermore, the paper emphasizes the importance of a coordinated response between technological means and the law, recommending the use of big data and artificial intelligence to improve the investigation and prevention of telecom fraud. The study suggests that only through the deep integration of legal frameworks and technology can the increasingly complex issue of telecom fraud in the digital society be effectively addressed.

Keywords

Digital society, telecom fraud, criminal law response, cross-border judicial cooperation, technological means

1. Introduction

The rapid advancement of information technology has made the digital society central to global economic and social operations. While networks and digital platforms offer convenience, they also foster the growth of new crimes, especially telecom fraud. This crime, characterized by its concealment, intelligence, and cross-border nature, challenges traditional legal systems in prevention and enforcement, threatening personal financial security and societal trust. China's criminal law has provisions against telecom fraud, but evolving methods make prosecution difficult, sentencing lenient, and cross-border enforcement challenging. With telecom fraud becoming globalized, international judicial cooperation and information sharing are crucial. This paper explores the state of telecom fraud, the limitations of current laws, and proposes measures to enhance legal adaptability, improve sentencing, and strengthen international cooperation. It also examines how technologies like big data and artificial intelligence can aid in fraud prevention and investigation, offering practical solutions to combat this growing issue (Barbosa, 2020, pp. 19-35).

2. The Current Situation and Characteristics of Telecom Fraud

2.1 Forms of Telecom Fraud in the Digital Society

In the digital society, the forms of telecom fraud have become increasingly diversified, with criminals constantly innovating their methods as technology advances. Common forms of telecom fraud include, but are not limited to, phone scams, SMS fraud, phishing, social media fraud, and cryptocurrency scams. These fraud schemes take advantage of the convenience of modern communication technology, quickly infiltrating people's daily lives. First, phone and SMS scams are the most traditional forms of telecom fraud. Criminals often impersonate government agencies, financial institutions, or other authoritative organizations, using intimidation or inducement to deceive victims into transferring money or providing sensitive personal information (Liu, 2021, pp. 1296-1316). Despite the simplicity of this approach, it remains one of the most common forms of fraud due to its wide reach and ease of operation. Second, with the development of the internet, phishing has become a significant tool in modern telecom fraud. Criminals create fake websites or send fraudulent emails to lure victims into clicking malicious links, thereby stealing personal information, account passwords, and more. This type of fraud is often closely linked to e-commerce platforms, payment systems, and other online services, causing victims to suffer financial losses without even realizing it. In addition, the rise of social media fraud and cryptocurrency scams marks new changes in telecom fraud in the digital age. Social media fraud typically involves criminals posing as celebrities or friends to carry out emotional scams or investment frauds (Zhang & Dong, 2023, p. 64). Cryptocurrency scams, on the other hand, exploit the anonymity and technical complexity of virtual currencies, setting up fake investment platforms to attract investors and ultimately profiting through "exit scams" or market manipulation. In summary, telecom fraud in the digital society is diverse and flexible. Criminals are adept at exploiting technological loopholes, legal gray areas, and people's trust in information authenticity, leading to the

rampant spread of fraud. This complexity poses significant challenges for the criminal justice system (Dong, 2023, pp. 59-65).

2.2 Characteristics of Telecom Fraud

Telecom fraud in the context of the digital society exhibits a set of unique characteristics, making criminal behavior more concealed, intelligent, and transnational, often on a large scale. Understanding these characteristics is crucial for an effective criminal law response. First, high concealment is one of the prominent features of telecom fraud. Criminals often use virtual identities and anonymous communication tools, such as virtual phone numbers, Virtual Private Networks (VPNs), or encrypted communication tools, making it difficult for victims to identify their real identities (Lentz & Nina, 2021, p. 1). At the same time, fraudsters hide the flow of funds by using multiple transfers or falsifying transaction records, further complicating investigation and tracking efforts. Second, telecom fraud has become increasingly intelligent and reliant on technology. Criminals are continually adopting advanced technological tools to enhance the complexity and targeting of their fraud schemes (Dumchykov, 2022, pp. 76-82). For example, they may use artificial intelligence to generate voice or video that mimics authoritative figures or relatives, making their fraud schemes more convincing. Additionally, through big data analysis, fraudsters can accurately target victims by analyzing personal information and behavioral patterns, executing highly tailored scams. This intelligence-driven fraud makes traditional prevention and tracking methods increasingly difficult. Third, telecom fraud shows a clear trend of transnationality and globalization. As global communication networks become increasingly interconnected, criminals can carry out fraud across borders, exploiting differences in laws and enforcement challenges between countries to evade legal accountability. For instance, criminals may plan and execute scams from one country, while victims and fund transfers occur in other nations, adding to the complexity and cost of combatting these crimes. Moreover, telecom fraud is often large-scale and organized. In recent years, many telecom fraud cases have been carried out by well-organized crime syndicates with clear divisions of labor, including specialized technical support, script training, and money laundering networks. These organized efforts enable fraud groups to simultaneously target large numbers of victims, causing significant social harm. Even more concerning, successful fraud techniques are quickly copied and spread by other criminal groups, further exacerbating the problem. In conclusion, the characteristics of telecom fraud—high concealment, intelligence, transnationality, and organized large-scale operations—make it increasingly difficult to prevent and combat in the digital society. These traits impose higher demands on the criminal justice system, which urgently requires legal and technological innovations to effectively tackle the growing complexity of telecom fraud.

3. Current Criminal Law Provisions for Telecom Fraud

3.1 Basic Criminal Law Provisions for Telecom Fraud

In addressing telecom fraud, current criminal law has established certain regulations and provisions. China's Criminal Law primarily deals with telecom fraud through the "crime of fraud" and related statutes. According to Article 266 of the Criminal Law of the People's Republic of China, fraud is defined as the act of illegally obtaining public or private property by fabricating facts or concealing the truth for the purpose of illegal possession. Depending on the amount involved, the law prescribes different levels of punishment, ranging from fixed-term imprisonment and detention to fines. In recent years, judicial interpretations have further clarified and supplemented the legal treatment of telecom fraud. For instance, the Supreme People's Court, Supreme People's Procuratorate, and the Ministry of Public Security have jointly issued several judicial interpretations targeting telecom fraud. These interpretations emphasize that, based on the fraud methods, the degree of harm, and the amount of money involved, corresponding convictions and sentencing should be applied. This ensures that even fraud carried out using the internet or communication technologies falls under the purview of the criminal law, thereby covering a wide range of telecom fraud activities. Additionally, China has introduced more stringent measures in recent years to combat telecom fraud (Ahmad et al., 2020, pp. 1308-1326). For example, the "Card Severing Action" launched in 2016 aimed to crack down on intermediaries that provide criminals with bank cards, mobile phone SIM cards, and other tools necessary for committing telecom fraud. Simultaneously, laws and regulations have gradually strengthened the supervision of third-party payment platforms, cryptocurrency exchanges, and other financial tools to reduce the avenues available for telecom fraud funds to be transferred. Although current criminal law offers a relatively clear framework for punishing telecom fraud, the diverse and rapidly evolving forms of telecom fraud pose challenges for the law in practice. For example, sentencing standards for fraud may not be fully adequate to deter large-scale, cross-border, and technology-driven telecom fraud. Additionally, the high degree of concealment involved in online fraud poses significant difficulties in evidence collection and prosecution under existing legal provisions. Therefore, while the current legal framework provides a basis for addressing telecom fraud, there is a need for further enhancement in its enforcement and adaptability to effectively combat the increasingly complex telecom fraud crimes in the digital society.

3.2 Gaps and Deficiencies in Criminal Law

Despite existing legal frameworks, significant gaps limit the effectiveness of combating telecom fraud, especially as these crimes become more complex and diverse. First, prosecution and evidence collection pose major challenges. Telecom fraud often involves the use of virtual identities, encrypted communications, and offshore servers, making it difficult to trace criminals. Fraudsters use virtual phone numbers, encrypted tools, and complex money transfers to hide their identities and obscure the flow of funds. The anonymity of online activities, combined with the cross-border nature of these crimes, complicates investigations and often requires international cooperation, which is slow and

complicated, hindering rapid responses and prosecutions. Second, sentencing standards are insufficient. Current laws base sentencing primarily on the monetary value of the fraud, but telecom fraud has broader social consequences, including societal disorder, public trust issues, and even national security threats. Large-scale fraud schemes often affect many victims, but the law's reliance on financial losses alone results in lighter sentences, reducing its deterrent effect. Third, inadequate international cooperation further hinders the prosecution of transnational fraud. Criminals exploit differences in laws and enforcement across countries to evade justice. Mechanisms for international cooperation remain underdeveloped, and differences in legal systems slow down efforts to combat fraud, making it difficult to prosecute and extradite suspects swiftly (McGuire, 2022, p. 35). Finally, the slow adoption of advanced technologies by law enforcement agencies limits their ability to combat increasingly sophisticated telecom fraud. While criminals use AI, big data, and other technologies to target victims, law enforcement often lacks the necessary tools to track real-time virtual currency transactions and freeze illicit funds. In conclusion, gaps in prosecution, sentencing, international cooperation, and technological adoption highlight the need for legal reforms, better international cooperation, and advanced technological tools to effectively address telecom fraud.

4. Criminal Law Approaches to Telecom Fraud in the Digital Society

4.1 Enhancing the Adaptability of Criminal Law in the Digital Age

In the digital society, telecom fraud is continuously evolving, requiring criminal law to be more flexible and adaptable to address the complexity and technical nature of these crimes. Strengthening the adaptability of criminal law has become a critical path for combatting telecom fraud. Firstly, revising and updating legal provisions is essential to improving the adaptability of criminal law. Due to the rapid evolution of fraud techniques, existing fraud-related legal provisions may not cover all emerging types of fraud. To address this challenge, criminal law needs to be updated to include more specific provisions for new forms of fraud prevalent in the digital society. For instance, new clauses should be added to address common forms of digital fraud such as cryptocurrency scams, phishing, and social media fraud. This would clarify the legal basis for prosecution and sentencing, enabling law enforcement to make swift legal judgments based on specific criminal behavior (Li & Yong, 2022, p. 4761230). Secondly, increasing the legal definition and penalties for technological crimes is crucial. As criminals use advanced technology to perpetrate fraud, criminal law must become more targeted in addressing technology-related crimes. Future laws should strengthen the legal definition of fraud using emerging technologies such as artificial intelligence and big data, especially in clarifying the responsibility of perpetrators using these tools. For example, laws should clearly define the criminal liability for fraud conducted via deep fake technology or synthetic voice technology and impose stricter penalties to create a strong deterrent effect. Additionally, enhancing the flexibility of legal interpretation is an effective way to improve the adaptability of criminal law. Given the fast pace of technological development, legislation often lags behind, making it difficult to revise laws in time to

cover all new forms of crime. Therefore, judicial authorities should apply legal interpretation more flexibly, interpreting and applying existing legal provisions to new types of crimes. For instance, in complex telecom fraud cases, judicial authorities can extend the interpretation of existing fraud provisions to cover new forms of cybercrime, ensuring that the law can respond flexibly to rapidly evolving technology. Finally, improving the coordination between criminal law and regulatory frameworks is essential. Telecom fraud in the digital society involves numerous technological tools and platforms. Criminal law must be closely integrated with regulatory mechanisms to adapt to the digital age. By collaborating with telecommunications operators, internet service providers, and payment platforms, a robust monitoring and early warning system can be established, effectively combining legal measures with technical regulation. For instance, laws can impose legal responsibilities on online platforms to take timely technical measures to block and report fraudulent activities, creating a synergy between legal and technical regulatory efforts. In summary, enhancing the adaptability of criminal law in the digital age is essential for combatting telecom fraud. Through revising and updating legal provisions, strengthening penalties for technological crimes, applying flexible legal interpretations, and improving coordination between law and regulatory frameworks, telecom fraud in the increasingly complex digital society can be more effectively addressed, ensuring the validity and authority of criminal law (Sinaga, 2023, pp. 4585-4604).

4.2 Improving the Determination of Criminal Liability and Sentencing

In addressing telecom fraud in the digital society, improving the determination of criminal liability and sentencing standards is a core measure for effectively combating these crimes. Current criminal law primarily bases sentencing for fraud on the amount of money involved, but as telecom fraud becomes more complex and socially damaging, the current sentencing system fails to fully reflect the severity and diversity of fraudulent activities. Therefore, it is necessary to optimize the determination of criminal liability and sentencing standards to enhance the specificity and deterrence of criminal law. Firstly, sentencing should consider the social harm caused by the crime. Telecom fraud not only results in financial losses but can also trigger public trust crises, social panic, and widespread societal issues. The current criminal law relies too heavily on the monetary amount of the fraud for sentencing and overlooks the broader social impact of the crime. For example, large-scale telecom fraud may involve relatively small individual losses but have a significant overall social impact. In such cases, sentencing should fully consider the social harm caused by the fraudulent activity and use it as an important factor in sentencing decisions. For cases that create widespread panic or damage public trust, even if the monetary amount is relatively low, penalties should be increased to strengthen deterrence. Secondly, differentiating the roles and responsibilities of participants is crucial in determining sentencing. In organized and transnational telecom fraud cases, participants often take on diverse roles, including planners, technical support, and fund transfer agents. Traditional fraud provisions do not adequately distinguish the varying degrees of involvement, leading to uniform sentencing standards. Improving the determination of criminal liability requires more precise differentiation of roles, with sentencing based

on each participant's specific involvement in the crime. For instance, planners and organizers of large-scale fraud should face more severe penalties, while technical support or fund transfer participants with lesser involvement should receive proportionate punishment, ensuring fair and reasonable sentencing. Additionally, introducing new sentencing standards to address technology-driven fraud is necessary. As telecom fraud increasingly relies on high-tech tools, the intelligence and technical complexity of fraudulent activities have escalated. Traditional sentencing standards based solely on the monetary value of the fraud are no longer sufficient to handle these sophisticated crimes. For example, criminals using phishing, malware, or artificial intelligence to commit fraud may cause large-scale personal information leaks in a short period, leading to significant potential risks for victims, even if no direct financial loss occurs. In such cases, criminal law should consider the unique nature of technology-driven fraud and introduce new standards for sentencing, such as the number of victims, the extent of information breaches, and the complexity of the fraudulent methods, allowing for a more comprehensive assessment of the social harm caused by the crime and appropriate sentencing. Finally, increasing penalties for transnational telecom fraud is essential. Transnational telecom fraud involves multiple jurisdictions, making law enforcement and accountability challenging. Therefore, criminal law should impose harsher penalties for transnational fraud to raise the cost of committing such crimes. For example, in addition to standard penalties, further sanctions could include banning perpetrators from engaging in certain industries, enhancing asset tracking and freezing, and increasing international criminal liability. By intensifying the penalties for transnational fraud, stronger legal deterrence can be created, preventing criminals from exploiting international legal differences to evade prosecution. In conclusion, improving the determination of criminal liability and sentencing is not only a legal safeguard against telecom fraud but also a crucial measure for enhancing the deterrent effect of criminal law and maintaining social order. By introducing more targeted sentencing standards, differentiating the roles and responsibilities of participants, adapting to the specific nature of technology-driven fraud, and increasing penalties for transnational crimes, criminal law can more effectively combat telecom fraud in the digital society and protect the legitimate rights and interests of the public.

5. The Role of International Cooperation and Technological Support in Combating Telecom Fraud

The cross-border nature and technological complexity of telecom fraud make it a global challenge, one that cannot be effectively addressed by the laws and enforcement mechanisms of any single country. Therefore, international cooperation and technological support play a crucial role in combating telecom fraud. Faced with these cross-border and high-tech crimes, countries must strengthen judicial cooperation and technical collaboration to jointly address this global security threat. First, international judicial cooperation is key to combating cross-border telecom fraud. Since telecom fraud often spans multiple countries and regions, criminals can easily exploit differences in legal systems and law

enforcement practices to evade prosecution. To effectively combat such crimes, countries need to establish tighter judicial cooperation mechanisms, promoting information sharing, evidence assistance, and international cooperation on extradition. For example, establishing a global unified telecom fraud database would help law enforcement agencies worldwide quickly access criminals' operational information and activity patterns, reducing their chances of fleeing across borders. Additionally, countries must enhance legal coordination in extradition procedures, simplifying the process to ensure that criminals are swiftly brought to justice. Second, technological support is a core tool in fighting telecom fraud. As fraud methods become increasingly intelligent and technologically advanced, traditional investigative techniques are no longer sufficient to deal with the complexity of modern telecom fraud. Therefore, law enforcement agencies worldwide must invest more in technological tools, utilizing Artificial Intelligence (AI), big data analytics, blockchain, and other advanced technologies to improve the detection and prevention of telecom fraud. For example, AI can help identify abnormal online activity and detect potential fraud, while big data can analyze vast amounts of network transactions and communication records to identify patterns of criminal behavior. Additionally, blockchain technology is particularly useful for tracking the flow of virtual currencies, aiding law enforcement in tracing the movement of fraudulent funds and freezing illegal assets, thereby undermining the financial foundation of criminal operations. In addition to international cooperation and technological support, the participation and coordination of international organizations are also indispensable. Global organizations such as Interpol and the International Telecommunication Union (ITU) play a crucial role in coordinating efforts to combat telecom fraud. These organizations provide platforms for technical support and information sharing among law enforcement agencies, helping countries increase the efficiency of their anti-fraud efforts. For example, Interpol has established a dedicated cybercrime unit responsible for coordinating anti-fraud actions among member countries and organizing multinational efforts to combat telecom fraud. This global cooperation improves the overall effectiveness of efforts to combat telecom fraud and helps curb the spread of these crimes. Lastly, the involvement of businesses and the public in providing technological support is also an essential part of combating telecom fraud. In addition to government cooperation, businesses and the public should actively participate in the fight against telecom fraud. Telecom operators, internet platforms, and financial institutions should strengthen their collaboration with governments by providing technical support and anti-fraud monitoring measures. For instance, telecom operators can intercept suspicious calls and messages through technical means, reducing the spread of fraudulent information; internet platforms can use AI to monitor user behavior, quickly identifying and blocking fraudulent accounts; and financial institutions should enhance monitoring and reporting mechanisms for suspicious transactions to prevent the rapid transfer of funds. At the same time, the public needs to raise awareness of fraud prevention, learn basic knowledge on how to avoid scams, and cooperate actively with government and corporate anti-fraud efforts. In summary, international cooperation and technological support play an irreplaceable role in combating telecom fraud. By strengthening international judicial

cooperation, leveraging advanced technological tools for investigation and prevention, and involving international organizations and the public, the global community can more effectively address the growing threat of telecom fraud, protecting citizens' financial security and maintaining social order.

6. Conclusion

In the context of the digital society, telecom fraud has become increasingly complex and transnational, presenting significant challenges to existing criminal law. Although laws have been established to address fraud, the constantly evolving techniques used in these crimes demand improvements in legal adaptability, sentencing standards, and mechanisms for international cooperation. By revising legal provisions, introducing new sentencing standards, enhancing international judicial collaboration, and leveraging technological tools such as big data and AI, we can more effectively combat telecom fraud and safeguard the public's financial security and social order.

References

Ahmad, A. H. et al. (2020). The impact of digitalization on occupational fraud opportunity in telecommunication industry: A strategic review. PalArch's *Journal of Archaeology of Egypt/Egyptology*, *17*(9), 1308-1326.

Barbosa, P. A. R. (2020). Corporate criminal law, artificial intelligence and Big Data: The huawei case and its implications for global society. *Revista Paradigma*, *29*(1), 19-35.

Dong, A. Y. (2023). The Characteristics and Prevention Countermeasures of Telecom Network Fraud Crime under the Background of Big Data. *Journal of Sociology and Ethnology*, *5*(5), 59-65.

Dumchykov, M. (2022). INTERNATIONAL LEGAL STANDARDS FOR COMBATING FRAUD IN THE FIELD OF COMPUTER INFORMATION. *European Socio-Legal and Humanitarian Studies*, *2*(2022), 76-82.

Lentz, L. W., & Nina, S. (2021). The use of historical call data records as evidence in the criminal justice system-lessons learned from the Danish telecom scandal. *Digital Evidence & Elec. Signature L. Rev.*, *18*(2021), 1. https://doi.org/10.14296/deeslr.v18i0.5235

Li, G., & Yong, W. (2022). [Retracted] Research on the Detection Countermeasures of Telecommunication Network Fraud Based on Big Data for Killing Pigs and Plates. *Journal of Robotics*, *2022*(1)), 4761230. https://doi.org/10.1155/2022/4761230

Liu, L. L. (2021). A jurisprudential analysis of the concurrent criminal jurisdiction over cross-border telecom fraud crime. *Journal of Financial Crime*, *28*(4), 1296-1316. https://doi.org/10.1108/JFC-09-2019-0123

McGuire, M. R. (2022). Crime, Control and the Ambiguous Gifts of Digital Technology. *The SAGE Handbook of Digital Society*, (2022), 35. https://doi.org/10.4135/9781529783193.n4

Sinaga, H. (2023). Legal and Ethical Implications in Data Theft Cases in the Digital Era. *East Asian Journal of Multidisciplinary Research*, *2*(11), 4585-4604. https://doi.org/10.55927/eajmr.v2i11.6791

Zhang, Y., & Dong, H. Y. (2023). Criminal law regulation of cyber fraud crimes—From the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*, *12*(1), 64. https://doi.org/10.1186/s13677-023-00437-3