Research On Laws, Regulations, And Policies of Internet Fraud

Angxiao Liu [1], Shien Piao [2, *]

[1] Beijing No.8 High School, Beijing, China

[2] Beijing International Bilingual Academy, Beijing, China

* Corresponding Author Email: 2024mpark@biba-student.org

Abstract. The purpose of this study is to explore the laws, regulations, and policies related to online fraud, in order to provide effective means to combat cybercrime. Given the increasingly rampant phenomenon of online fraud, research on relevant laws, regulations, and policies has become particularly important. In the research background, this article first introduces the definition, form, and harm of online fraud. The research subjects include relevant legislation and policy documents on online fraud both domestically and internationally, as well as legal cases and practical experience in recent years. Through the sorting and analysis of these materials, this article summarizes the main laws, regulations, and policy measures for the prevention and control of online fraud. The research results show that various countries and regions have taken various measures to combat online fraud, including formulating specialized laws on cybercrime, improving criminal law systems, and establishing cross-border cooperation mechanisms. At the same time, the government, enterprises, and individuals should work together to strengthen cybersecurity education and technological prevention, in order to improve their ability to identify and prevent online fraud. In summary, this study conducted a comprehensive investigation and analysis of the laws, regulations, and policies related to online fraud, providing strong support for the development of more sound measures for preventing and controlling cybercrime. Further research and practice will help effectively respond to the constantly changing situation of online fraud, and protect social cybersecurity and public interests.

Keywords: Crime; regulation; Internet; government.

1. Introduction

With the progress of the Internet and science and technology, modern society has a great development and changes. The Internet gives people more convenient communication and work efficiency and improves people's quality of life. Society is progressing and people are getting richer. But the Internet is double face. there are telecom fraud and network crime. Now through the intrusion of computer networks, telecom fraud has become a serious threat to social security and economic development. In this regard, the study of Internet crime behavior can effectively identify the law of fraud crime and more effectively reduce the number of victims. By understanding the law of fraud, we can reverse the management of fraudsters, find the criminal base, and solve the criminal organization. In the face of cybercrime, people adopt network investigation to study criminal activities, mainly using mobile digital forensics and open-source intelligence investigation. Among them, extracting logical language and hexadecimal are the main tools for data investigation, while open-source intelligence focuses on the use of natural language. In another approach, online surveys, investigators use many sources of information when conducting online surveys. The three main sources are the open Web, the deep Web, and the dark web. Among them, the dark web is a subset of the deep web rather than a separate source of information. Researchers are always applying new techniques in open-source intelligence and online surveys in order to gain as much intelligence as possible on fraudsters. Each of these methods provides some information, but none of them provides the information needed for the investigation. However, natural language processing can be applied to many different cases and provide investigators with several different types of information [1].

2. Overview of Internet Fraud

2.1. Definition

Online fraud refers to the act of using deceptive means to illegally obtain property, information, or other improper benefits from others in the online environment [2]. The characteristics of online fraud include:

1. False identity: Fraudsters usually use false identity information or impersonate others' identities to gain the trust of victims.

2. Deception methods: Common online fraud methods include false claims of winning prizes, false investments, counterfeit websites, counterfeit goods, phishing emails, etc., with the aim of deceiving victims to obtain money or sensitive information.

3. Concealment: Online fraud is often carried out through online platforms, allowing fraudsters to hide their identity and whereabouts, making it difficult to pursue and causing greater distress to victims.

2.2. Features

Online fraud can be divided into various types, and the following are some common classifications:

(1) Phishing fraud: Inducing victims to provide personal or bank account information by forging legitimate institutions' websites or sending false emails.

(2) Lottery fraud: False notification to the victim that they have won the lottery or lottery, and demand that the victim pay the relevant fees in order to receive the bonus.

(3) Investment fraud: Under the guise of illegal investment, luring victims to invest in fake projects, promising high returns, and ultimately deceiving victims of their money.

(4) Online shopping fraud: Under the guise of low-priced products or counterfeit brands, false transactions are carried out to deceive consumers into paying, and then not shipping or distributing counterfeit goods [3].

(5) Understanding fraud: Using social media platforms or dating websites to establish relationships through false identities, and then using methods such as seeking help, borrowing money, and investing in projects to defraud victims of their property.

The above are only some common categories of online fraud, and fraudsters will constantly change their tactics and strategies. Therefore, it is necessary to remain vigilant and improve their own network security awareness. When encountering suspicious situations, it is necessary to promptly report to relevant departments to avoid losses. It should be noted that the tactics of online fraudsters are constantly changing and updating, and they will continuously improve their fraud methods to adapt to new network technologies and user behavior. Therefore, it is very important to remain vigilant, enhance network security awareness, and timely understand and master the latest online fraud techniques and preventive measures.

3. Current Situation and Trend

3.1. Overview of Global Network Fraud Incidents and High-Incidence Countries

Currently, online fraud has become a serious problem worldwide, causing huge economic and social losses to individuals, businesses, and society. Online fraud cases are constantly emerging, and various new forms of fraud are constantly emerging, making the task of combating online fraud increasingly challenging.

On a global scale, online fraud incidents are constantly increasing and becoming increasingly complex. According to statistical data, in recent years, there has been a significant increase in fraud cases worldwide. Financial fraud, online shopping fraud, investment fraud, and phishing emails have become the main types of online fraud. The continuous innovation of fraud methods, including

phishing websites, deceiving phone calls, and false SMS, has caused great distress to users. A typical case of website fraud in the UK is Des Dillon, who runs a student accommodation company, telling BBC 5 Live that he was deceived into leaking information, resulting in a loss of £ 230000 in the company's bank account and becoming a victim of cybercrime [4].

In high-risk areas, several countries are particularly prominent. Developed countries such as the United States, the United Kingdom, Canada, and Australia are popular areas with high incidences of online fraud. These countries have developed financial and internet industries, and personal information, property, and electronic payments are relatively popular. It is precisely these factors that have led to the high incidence of online fraud in these regions [5]. In addition, some developing countries are gradually becoming high-risk areas for online fraud. Due to the popularization of internet access and the improvement of payment systems, individuals and enterprises are more susceptible to attacks in the network environment. Especially in some economically weak areas, people have relatively low awareness of network security and are prone to becoming victims of online fraud.

3.2. Future Trend

In the future, the trend of online fraud will present the following characteristics:

Firstly, with the popularization of the Internet and the continuous progress of technology, online fraud methods will become more complex and covert. Fraudsters will pay more attention to carefully creating fake websites, forging identities and information, and using technical means to obtain user personal information and account passwords. Secondly, the popularity of mobile payments will make mobile network fraud a new risk point. The increasing popularity of mobile devices provides more opportunities for fraudsters. Fake apps, phishing messages, and other methods will become new hotspots of online fraud. Finally, the joint efforts of multiple countries to combat online fraud will become an important trend. With the increasing cross-border nature and complexity of online fraud, cooperation between countries will become closer. Through international cooperation to jointly combat online fraud, it will help reduce the occurrence of online fraud.

In order to address the challenges of online fraud, individuals and businesses should strengthen their awareness of network security, improve their ability to identify risks, and not trust strangers' information and links. At the same time, governments of various countries should take effective measures to strengthen the construction of laws and regulations and strengthen international cooperation to jointly combat online fraud and maintain network security. Only with the joint efforts of the whole society can we effectively prevent and combat online fraud.

4. Internet Fraud Laws and Regulations in China

4.1. Provisions on Online Fraud in the Chinese Criminal Law

In order to manage the fraud crime and punishment, the national government issued a series of laws and regulations, to sanction and deal with the crime. Article two hundred and sixty-six in criminal law, for example, "fraud" fraud public or private property, relatively large, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance, and concurrently or independently be sentenced to a fine.

If the amount involved is especially huge, or if there are other serious circumstances, he shall be sentenced to fixed-term imprisonment of not less than 10 years or life imprisonment and shall also be fined or sentenced to confiscation of property. According to the interpretation of the Supreme People's Court on several issues concerning the specific application of the law in the trial of fraud cases: individuals defrauding public and private property of more than 2,000 yuan, belonging to the "large amount"; Individual fraud public or private property over 30000 yuan, belong to "huge" [6].

4.2. Other Relevant Legal Provisions

At the same time, as stipulated in the criminal law if someone frauds public or private property worth 200000 yuan or above, belongs to the amount is especially huge. The amount of fraud is particularly huge, identified fraud crime "particularly serious circumstances" an important feature, but not the only feature. Such as the amount is 100,000 yuan or above, but also has one of the following circumstances, defined as: "if the circumstances are especially serious."

(1) the fraud group ringleaders or common fraud crime is serious in the principal.

(2) Repeat offenders or fugitives who commit crimes with serious harm.

(3) defrauding legal persons, other organizations, or individuals of the means of production urgently needed, seriously affecting production or causing other serious losses.

(4) fraud disaster relief, emergency rescue, flood prevention and control, materials, relief, medical sources, thereby causing serious consequences.

(5) squandering the defrauded property so that the defrauded property cannot be returned.

(6) using fraudulent property to carry out illegal and criminal activities.

(7) having been subject to criminal punishment for fraud.

(8) causing death, mental disorder, or other serious consequences to the victim.

(9) other serious circumstances. If the directly responsible person in charge of the unit or other directly responsible persons commits fraud in the name of the unit and the proceeds of fraud belong to the unit, and the amount of fraud is between 50,000 yuan and more than 1,000 yuan, the above-mentioned persons shall be investigated for criminal responsibility in accordance with the provisions of Article 152 of this Law; Amount in more than 200000 yuan to 300000 yuan, in accordance with the provisions of article l52 shall be investigated for criminal responsibility of the staff [7].

Under these strong laws and regulations, fraud has declined, and more activity has taken place outside China. Laws and regulations formulated by the government have a certain deterrent power and stabilize the public order of society.

4.3. Problems and Deficiencies in Current Laws and Regulations

There are a series of problems and deficiencies in China's current fraud laws and regulations. Firstly, the legal definition is unclear. The definition of fraud is not clear, leading to disputes over the application of legal provisions. The blurry boundary between fraud and other similar crimes makes it difficult and uncertain for relevant law enforcement agencies to determine and hold accountable. This provides some criminals with an opportunity to evade legal sanctions. Secondly, the difficulty of proving is relatively high. When dealing with fraud cases, victims need to provide a large amount of evidence to prove their losses and the fact of being deceived. However, fraudsters often use technical means to conceal criminal behavior, making it difficult for victims to provide evidence. One of the main problems is a lack of clear definitions of corporate fraud, which can lead to confusion and uncertainty among companies and regulators. The increase in the difficulty of proof provides fraudsters with the opportunity to evade sanctions and also gives victims a greater blow.

Furthermore, online fraud usually involves cross-border crimes, making law enforcement significantly more difficult. Noting that regulators may lack the necessary resources and capabilities to detect and prosecute cases of fraud effectively. This can be particularly problematic in cases where fraudulent activities are complex or involve overseas entities, as coordinating investigations across borders can be challenging. The lack of effective international cooperation mechanisms and information sharing has constrained the effectiveness of combating transnational cyber fraud crimes. This also provides criminals with the opportunity to take advantage of differences in legal systems and covert behavior in different countries, allowing them to evade sanctions.

Overall, the paragraph provides a clear and insightful summary of some of the key problems and shortcomings of China's current fraud laws and regulations. By highlighting these issues, it suggests that there is significant room for improvement in this area and that more needs to be done to ensure that China's legal framework for addressing corporate fraud is effective in deterring and punishing offenders.

5. International Legal Cooperation on Internet Fraud

5.1. International Network Fraud Cases and Cooperation Mechanisms

At the same time, network fraud is always frequent in the world, people in different countries have received network telecom fraud. The phenomenon of transnational crime seriously affects the stable environment of the international society. Therefore, every country has set up some relevant regulations to protect the legitimate rights and interests of people. Rampant fraud, in addition to technology and network anonymity, there is a very important reason is that transnational crime, because of the differences in national legal system, also the lack of a fixed cooperation way, lead to international telecom fraud cases of complex and difficult to track down and prosecute. So in addition to the establishment of legal provisions in each country, the international also takes a cooperative way to combat network telecom fraud.

5.2. Investigation of International Cyberfraud Cases

For example, on August 23, 2023, according to the Chinese Embassy in Myanmar, six telecom fraud suspects were handed over by the Myanmar police to the Chinese police working group at Yangon International Airport in two batches for an escort back home [8]. This is the second time after the six suspects of electricity fraud in Myanmar were escorted back to China in June this year. Police in China, Thailand, Myanmar, and Laos have launched a joint campaign to crack down on telecom and Internet fraud and online gambling crimes in the region.

At the same time, on August 29, Chinese and Indonesian police organized the first batch of centralized network closing operations, entered the Indonesian Batam island of large telecom network fraud crime centers, successfully arrested 88 telecom network fraud suspects, the scene seized more than 80 computers, more than 200 mobile phones and a large number of bank cards and other crime tools. According to a preliminary investigation, more than 40 naked chat extortion cases involving many places in China were carried out by this criminal gang, and relevant cases are being further investigated. At present, the Indonesian police have agreed to transfer the criminal suspect, our Ministry of Public Security organization in the near future civilian police to 88 suspects sent home.

After the deepening of international cooperation, transnational network fraud gradually reduced, effectively protecting the legitimate rights and interests of the people. At the same time, international laws and regulations and international cooperation have deepened the ties between countries and jointly maintained the stability of the international community.

6. Prevention and Combat Policy

6.1. The Responsibilities and Roles of Government Departments

With the popularization of the Internet and the development of digital society, online fraud has increasingly become a criminal behavior that endangers social security and personal interests. Faced with the increasingly rampant crime of online fraud, the government must take effective preventive and crackdown measures to safeguard the rights and interests of citizens and social stability. This article will elaborate on the roles and responsibilities of government departments, institutional construction, and information security education and awareness enhancement.

6.2. Institutional Construction to Prevent and Combat Online Fraud

Firstly, the government plays an important role and responsibility in preventing and combating online fraud. The government should strengthen supervision and law enforcement, formulate and improve relevant laws and regulations, and ensure their effective implementation. By increasing the crackdown on online fraud, we can effectively curb the arrogance of criminals and maintain social order. In addition, the government should also strengthen cooperation among various departments, establish cross-departmental and cross-regional cooperation mechanisms, and form a strong

crackdown force. All relevant departments should strengthen cooperation, share intelligence, and promptly detect and prevent online fraud activities. Secondly, the government should strengthen technological research and innovation, and improve its ability to identify and analyze online fraud technologies. Cyber fraud often utilizes advanced technological means and means, which puts higher demands on the government's ability to counter it. The government should strengthen the cultivation and introduction of technical personnel, provide advanced technical equipment and tools, and improve the rapid response ability to online fraud. In addition, the government should also increase supervision and guidance on the network security industry and encourage enterprises to improve their security protection level. On the other hand, institutional construction is an important guarantee for preventing and combating online fraud. The government should establish institutions for reporting and accepting online fraud, provide convenient reporting channels, and keep whistle blowers confidential and rewarded. By building an effective reporting platform, it is possible to quickly receive and process reporting information about online fraud, making it easier to crack down on criminals. At the same time, the government should also establish a credit evaluation system to punish those suspected of online fraud, and through severe crackdowns on criminals, play a deterrent role in reducing the occurrence of online fraud. In the opinion on strengthening the crackdown on illegal and criminal activities related to telecommunications network fraud issued by the General Office of the State Council, it is stated that it is necessary to strictly crack down on illegal and criminal activities related to telecommunications network fraud in accordance with the law. We need to build a strict prevention system, strengthen technical countermeasures, and establish anti-fraud websites, apps, and fraudulent phone calls. And strengthen industry supervision and source governance. Establish and improve industry safety assessment and admission systems [9]. In addition, the government should also increase efforts in information security education and awareness enhancement for the public. The public's awareness and vigilance towards online fraud determine the security of individuals and society. The government should strengthen publicity and training, increase public awareness and understanding of online fraud, and help them identify and respond to various types of online fraud methods. At the same time, the government should also strengthen network security education for teenagers, cultivate their awareness and ability to use the internet correctly and prevent them from becoming victims of online fraud [10].

In short, the prevention and crackdown on online fraud is a complex process that requires the joint efforts of the government, enterprises, and individuals. The government should strengthen supervision and law enforcement, strengthen cooperation, increase investment in technology research and development, establish institutions for reporting and accepting online fraud, and improve institutional construction. At the same time, the government should also increase its efforts in information security education and awareness enhancement and raise the public's and young people's awareness about network security. Only through the joint efforts of the government, enterprises, and individuals can a safe and healthy cyberspace be established to jointly resist the threat of online fraud.

7. Conclusion

Online fraud is a criminal behavior that has rapidly developed with the popularity of the Internet in recent years, causing serious losses to individuals, businesses, and society. In order to maintain network security and combat online fraud, countries have formulated laws, regulations, and policies targeting cybercrime. Many researchers have conducted extensive research and achieved some important results. However, I need more specific information to construct a summary of the research results of a research paper. The information currently provided and searched online is not sufficient to represent online fraud. During the process of reading and analysis, there may be times when there is insufficient support for paragraph arguments. This article will evaluate the laws, regulations, and policies related to online fraud and provide recommendations.

Firstly, for the laws and regulations of online fraud, countries generally adopt a combination of criminal punishment and civil compensation. Criminal punishment can serve as a deterrent and punish

criminals who commit online fraud; Civil compensation can protect the legitimate rights and interests of victims and enable them to obtain economic compensation. However, current methods of online fraud are constantly emerging, and laws and regulations are relatively lagging, making it difficult to investigate and handle new types of online fraud. Therefore, it is suggested that the formulation of laws and regulations should follow the development of the times and strengthen the standardization of new types of online fraud methods. Secondly, policies regarding online fraud mainly include national policies and regulations on corporate self-discipline. National policies, including strengthening network security supervision and enhancing technological prevention capabilities, can provide policy support for combating online fraud. The regulations on self-discipline in enterprises aim to cultivate standardized behavior among users, emphasizing the creation of a healthy online environment. However, due to the cross-border, anonymous, and technical nature of online fraud, international cooperation is needed to jointly combat online fraud crimes. Therefore, it is recommended to strengthen international cooperation and strengthen global governance of online fraud through information sharing, cooperation, and other means. In addition, the evaluation of laws, regulations, and policies related to online fraud also requires attention to law enforcement efficiency and the rationality of criminal law sentencing. The investigation and prosecution of online fraud cases require a combination of technical means and legal intelligence, but due to the complexity of technology and practical limitations, the efficiency of law enforcement is still relatively low. The rationality of criminal law sentencing is also an urgent issue that needs to be improved. The law adopts unified criminal law sentencing standards for different types of online fraud crimes, which may lead to cognitive differences in criminal behavior. Therefore, it is recommended to strengthen the training and technical support of law enforcement forces, while moderately adjusting the sentencing standards of the criminal law to ensure an effective crackdown on online fraud crimes.

In summary, online fraud laws, regulations, and policies have played an important role in combating online fraud, but they still face difficulties in responding to new forms of online fraud and cross-border crackdowns. Therefore, it is recommended to formulate laws and regulations that keep up with the times, strengthen international cooperation, improve law enforcement efficiency, and the rationality of criminal law sentencing to maximize the maintenance of network security and combat online fraud crimes. At the same time, we will strengthen public education on network security awareness, cultivate user behavior norms, and jointly create a good network environment.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Fortinet. What is internet fraud? Types of internet fraud? Retrieved form https://www.fortinet.com/resources/cyberglossary/internet-fraud#:~:text=The%20term%20%22internet%20fraud%22%20generally,scam%20people%20out%20of%20money.

[2] Cyberfraud. 2023. Retrieved form https://dictionary.cambridge.org/dictionary/english/cyberfraud.

[3] TSB Bank. Business Talk: The common types of cyber fraud and how to detect them, 2022. Retrieved form https://www.tsb.co.uk/business/business-talk/the-common-types-of-cyber-fraud-and-how-to-detect-them/

[4] BBC News. Cybercrime and fraud scale revealed in annual figures. 2019, Retrieved form https://www.bbc.com/news/uk-38675683

[5] Global fraud report 2022. Retrieved form https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2022.pdf

[6] What are the legal provisions for online fraud and what are the legal provisions? 2023, Retrieved form https://v.66law.cn/wenda/1148009.

[7] What are the regulations for online fraud? 2023, Retrieved form https://www.64365.com/zs/816039.aspx.

[8] International cooperation is crucial in combating cross-border electronic fraud. 2023, Retrieved form https://baijiahao.baidu.com/s?id=1775099228022504625&wfr=spider&for=pc.

[9] Yu Zhu. The General Office of the Central Committee of the Communist Party of China and the General Office of the State Council have issued the "Opinions on Strengthening the Crackdown on and Governance of Illegal Telecommunications Network Fraud Crimes". 2022, Retrieved form https://www.gov.cn/zhengce/2022-04/18/content_5685895.htm?eqid=ebc6643600002b54000000036492a306.

[10] Cybercrime and fraud prevention for your home, office, and clients. Retrieved form https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2017/september-october/cyber-crime-fraud-prevention/.